ARGUMENT NOT YET SCHEDULED

No. 18-1051 (Lead)

***Consolidated with Nos* 18-1052, 18-1053, 18-1054, 18-1055, 18-1056, 18-1061, 18-1062, 18-1064, 18-1065, 18-1066, 18-1067, 18-1068, 18-1088, 18-1089, 18-1105**

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

MOZILLA CORPORATION et. al.,

Petitioners,

v.

FEDERAL COMMUNICATIONS COMMISSION
AND UNITED STATES OF AMERICA,

Respondents.

On Petition for Review of an Order
of the Federal Communications Commission

AMICUS BRIEF OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PETITIONERS

Mitchell Stoltz
Corynne McSherry
Kit Walsh
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Attorneys for Amicus Curiae

CERTIFICATE AS TO PARTIES, RULINGS, RELATED CASES, AND STATUTES

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

All parties, intervenors, and amici appearing before this Court are listed in the Joint Brief of Non-Government Petitioners and the Proof Brief for Government Petitioners. Those briefs also provide a lengthy, but nonexhaustive, listing of participants before the FCC in the proceeding under review.

B. Rulings Under Review

The ruling under review is the FCC's, Declaratory Ruling, Report, and Order, and Order *In the Matter of Restoring Internet Freedom*, 33 F.C.C. Rcd. 311 (2018).

C. Related Cases

The ruling under review has not been and is not the subject of any other petition for review, aside from those actions that have been consolidated in this proceeding.

Prior FCC rulings concerning protections for the open Internet have been reviewed by this Court and would be substantially eliminated by the ruling under review. The FCC's 2010 order, *In the Matter of Preserving the Open Internet*, Report and Order, 25 F.C.C. Rcd. 17905 (2010), was affirmed in part and vacated

in part in *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014). The F.C.C.'s 2015 order, *In the Matter of Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 F.C.C. Rcd. 5601 (2015), was affirmed in *U.S. Telecom Ass'n v. FCC*, 825 F.3d 674 (D.C. Cir. 2016). This Court denied a petition for rehearing en banc. *U.S. Telecom Ass'n v. FCC*, 855 F.3d 381 (D.C. Cir. 2017).

The following cases involve pending petitions to the Supreme Court for certiorari from the aforementioned U.S. Telecom proceeding:

Daniel Berninger v. FCC, S.Ct. No. 17-498

AT&T Inc. v. FCC, S.Ct. No. 17-499

American Cable Ass'n v. FCC, S.Ct. No. 17-500

CTIA-The Wireless Ass'n v. FCC, S.Ct. No. 17-501

NCTA-The Internet & TV Ass'n v. FCC, S.Ct. No. 17-502

TechFreedom v. FCC, S.Ct. No. 17-503

United States Telecom Ass'n v. FCC, S.Ct. No. 17-504

D. Statutes and Regulations

All applicable statutes, etc., are contained in the Brief for Government Petitioners, filed August 20, 2018.

August 27, 2018

/s/ Mitchell Stoltz
Mitchell Stoltz

CORPORATE DISCLOSURE STATEMENT

Pursuant to D.C. Circuit Rule 26.1 and Federal Rule of Appellate Procedure 26.1, *amicus* submits 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.

TABLE OF CONTENTS

CERTIFICATE AS TO PARTIES, RULINGS, RELATED CASES, AND STATUTES i

CORPORATE DISCLOSURE STATEMENT iii

TABLE OF AUTHORITIES vi

GLOSSARY OF ABBREVIATIONS xi

INTEREST OF AMICUS 1

INTRODUCTION AND SUMMARY OF ARGUMENT 3

ARGUMENT 6

I. The Restoring Internet Freedom Order Is Arbitrary and Capricious Because It Misunderstands BIAS Providers' Offerings. 6

A. BIAS Providers Offer Access to Content and Services on the Internet—Not the Content and Services Themselves. 8

B. The Domain Name System Is Not an Integral Part of a BIAS Offering. 9

C. Caching Is a Non-Essential and Increasingly Obsolete Practice. 12

D. DNS and Caching Are Not Information Services. 15

II. The 2018 Order Is Arbitrary and Capricious Because It Fails to Address the Detrimental Impact on Online Speech and Innovation. 16

A. Net Neutrality Was Built Into the Design of the Internet and Made the Internet Into a Powerhouse for Speech and Innovation. 16

B. It Is Arbitrary and Capricious to Ignore the Danger the 2018 Order Poses for Speech and Innovation Online. 20

C. It Is Arbitrary and Capricious to Conclude that Consumer Choice Can Fix these Problems. 25

CONCLUSION 29

CERTIFICATE OF COMPLIANCE 31

CERTIFICATE OF SERVICE.....32

APPENDIX A.....33

TABLE OF AUTHORITIES

Cases

Allentown Mack Sales and Service, Inc. v. NLRB,
522 U.S. 359 (1998).....7

In the Matter of Amendment of Section 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry),
77 F.C.C.2d 384 (1980).....17

In the Matter of MTS and WATS Market Structure,
97 F.C.C.2d 682 (1983) 18

In the Matter of Proposals for New or Revised Classes of Interstate and Foreign Message Toll Telephone Service (MTS) and Wide Area Telephone Service (WATS),
56 F.C.C.2d 593 (1975).....17

In the Matter of Protecting and Promoting the Open Internet,
30 F.C.C. Rcd. 5601 (2015).....3

In the Matter of Restoring Internet Freedom,
33 F.C.C. Rcd. 311 (2018) 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 20, 21, 22, 23, 24, 25, 26, 28, 29

Int'l Union, United Mine Workers v. Mine Safety & Health Admin.,
626 F.3d 84 (D.C. Cir. 2010).....7

Michigan v. EPA,
135 S. Ct. 2699 (2015).....29

**Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*,
463 U.S. 29 (1983).....7, 29

Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs.,
545 U.S. 967 (2005).....9

Packingham v. North Carolina,
137 S. Ct. 1730 (2017).....4

**Red Lion Broad. Co. v. FCC*,
395 U.S. 367 (1969).....27

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

U.S. Telecom Ass'n v. FCC,
825 F.3d 674 (D.C. Cir. 2016) 28

Verizon v. FCC,
740 F.3d 623 (D.C. Cir. 2014) 28

Statutes

*47 U.S.C. § 153 (2018) 6, 15

5 U.S.C. § 706 7

Legislative Materials

*H.R. Rep. No. 102-850 (1992) 18

Other Authorities

@WhiteHouse, Twitter, https://twitter.com/whitehouse 4

1.1.1.1—the Internet's Fastest, Privacy-First DNS Resolver, Cloudflare,
https://cloudflare-dns.com/ 11

2018 Broadband Deployment Report, FCC (Feb. 2, 2018),
https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2018-broadband-deployment-report 4

Aaron Pressman, *The Cable TV Industry Is Getting Even Less Popular*,
Fortune (May 25, 2017), https://fortune.com/2017/05/25/cable-tv-comcast-verizon/ 9

Adam Liptak, *Verizon Blocks Messages of Abortion Rights Group*,
N.Y. Times (Sept. 27, 2007), https://www.nytimes.com/2007/09/27/us/27verizon.html 22

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), https://alissacooperdotcom.files.wordpress.com/2017/12/chapter6-final.pdf 21

AT&T Calls Censorship of Pearl Jam Lyrics an Error, Reuters (Aug. 9, 2007),
https://www.reuters.com/article/technologyNews/idUSN091821320070809.....22

B. Carpenter, *Request for Comments 2775: Internet Transparency*, "The end-to-end argument," IBM (2000), https://tools.ietf.org/html/rfc2775 #section-2.1 20

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), http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf 21

CIDR Report for 20 Aug 18, CIDR Report, http://www.cidr-report.org/as2.0/ 18

Cloud Delivered Enterprise Security by Open DNS, CISCO, https://www.opendns.com/ 11

*Dan Goodin, *New Firefox Version Says "Might as Well" to Encrypting All Web Traffic*, Ars Technica (Apr. 1, 2015), https://arstechnica.com/security/2015/04/new-firefox-version-says-might-as-well-to-encrypting-all-web-traffic/ 15

Data Networks and Open System Communications; Open Systems Interconnection—Model and Notation, International Telecommunication Union (July 1994), https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.200-199407-I!!PDF-E&type=items.....19

David D. Clark, *The Design Philosophy of the DARPA Internet Protocols*, ACM SIGCOMM Computer Comm. Rev., Vol. 18, Aug. 1988 20

Domain Hosting & Email Services, https://www.sonic.com/business/hosting.....11

Domain Name System (DNS) Services – Verizon ROUTE, https://www.verizondigitalmedia.com/platform/route/ 11

E-mail from Eric Rescorla to TLS mailing list (Oct. 6, 2017, 20:17 CST), https://mailarchive.ietf.org/arch/msg/tls/yt4otPd5u_6fOzW02TEe2e-W5G0 23

Evan Anderson, *Fixing Charter's DNS Hijacking*, Evan J.D. Anderson (June 23, 2010), https://ejdanderson.wordpress.com/2010/06/23/fixing-charters-dns-hijacking/.....12

Firefox & Page Load Speed – Part II (Apr. 5, 2010), https://blog.mozilla.org/metrics/2010/04/05/firefox-page-load-speed---part-ii/.....24

*Gennie Gebhart, *We're Halfway to Encrypting the Entire Web*, Electronic Frontier Foundation (Feb. 21, 2017), https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web 14

High Speed Internet Service from XFINITY by Comcast, https://www.xfinity.com/learn/internet-service 10

*Ian Austen, *A Canadian Telecom's Labor Dispute Leads to Blocked Web Sites and Questions of Censorship*, N.Y. Times (Aug. 1, 2005), https://www.nytimes.com/2005/08/01/business/worldbusiness/a-canadian-telecoms-labor-dispute-leads-to-blocked.html 21

Internet Access Services: Status as of December 31, 2016, FCC (Feb. 2018), https://docs.fcc.gov/public/attachments/DOC-349074A1.pdf 27

Internet/Broadband Fact Sheet, Pew Research Center, http://www.pewinternet.org/fact-sheet/internet-broadband/ 4

J.H. Saltzer et al., *End-to-End Arguments in System Design*, ACM Transactions on Computer Sys., Vol. 2, Nov. 1984 20

James A. Gardner, *Anonymity and Democratic Citizenship*, 19 Wm. & Mary Bill Rts. J. 927 (2011), http://scholarship.law.wm.edu/wmborj/vol19/iss4/6/ 5

Jason Oxman, *The FCC and the Unregulation of the Internet* 17 (FCC Office of Plans and Policy, Working Paper No. 31, July 1999), https://www.fcc.gov/Bureaus/OPP/working_papers/oppwp31.doc 17

Julius Genachowski, Chairman, FCC, *Remarks at the Joint Center for Political and Economic Studies: Media & Technology Policy Forum* (Mar. 3, 2010), https://www.fcc.gov/events/speech-open-internet-innovation-and-economic-development 5

Message from the Internet Architecture Board to Stuart Lynn, ICANN (Jan. 25, 2003), https://www.icann.org/resources/pages/iab-message-to-lynn-2003-01-25-en 12

Quad9 DNS: Internet Security and Privacy in a Few Easy Steps, https://quad9.net/ 11

Ryan Singel, *ISPs' Error Page Ads Let Hackers Hijack Entire Web, Researcher Discloses*, WIRED (Apr. 19, 2008), https://www.wired.com/2008/04/isps-error-page 12

Samuel Stebbins et al., *Bad Reputation: America's Top 20 Most-Hated Companies*, USA Today (Feb. 1, 2018), https://www.usatoday.com/story/money/business/2018/02/01/bad-reputation-americas-top-20-most-hated-companies/1058718001/ 9

Sarah Almukhtar et al., *Black Lives Upended by Policing: The Raw Videos Sparking Outrage*, N.Y. Times, https://www.nytimes.com/interactive/2017/08/19/us/police-videos-race.html 5

Services | Viasat, https://www.viasat.com/services 10

U.S. Dep't of State, Alerts and Warnings, https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html 4

Vinton G. Cerf and Robert E. Kahn, *A Protocol for Packet Network Intercommunication*, IEEE (1974), https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf.....19

Vishal Misra, *Net Neutrality Is All Good and Fine; The Real Problem Is Elsewhere* (2014), https://www.cs.columbia.edu/2014/net-neutrality/ 29

Yunhong Gu, *Google Public DNS and Location-Sensitive DNS Responses*, Google Webmaster Central Blog (Dec. 15, 2014), https://webmasters.googleblog.com/2014/12/google-public-dns-and-location.html 11

GLOSSARY OF ABBREVIATIONS

BIAS: Broadband Internet Access Service

CDN: Content Delivery Network

DNS: Domain Name System

ISP: Internet Service Provider

TLS: Transport Layer Security

INTEREST OF AMICUS[1]

EFF is a member-supported nonprofit organization devoted to protecting civil liberties and free expression in technology, law, policy, and standards. With over 40,000 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 and TMobile's 2016 throttling of video streams.

EFF files this brief on behalf of technologists who have helped develop core Internet technologies. See Appendix A for the full list of 130 names. As architects of the Internet who are justly proud of their creation, they are deeply

[1] No party's counsel authored this brief in whole or in part. No party or party's counsel, nor any person besides *amicus*, its members, or its counsel contributed money toward this brief. Counsel for all parties and intervenors have consented to, or indicated that they do not oppose, the filing of this brief. EFF thanks legal intern Edward Nugent for his valuable contributions to this brief, and, in the interest of full disclosure, notes that he previously counseled Petitioner Santa Clara County in this matter prior to becoming an intern at EFF.

concerned that the FCC is abdicating its traditional role in protecting net neutrality, particularly given that its decision is based on a fundamentally flawed understanding of how the Internet works.

INTRODUCTION AND SUMMARY OF ARGUMENT

Developers of the Internet are deeply concerned that the Federal Communications Commission ("FCC") has improperly and dangerously reversed net neutrality protections and principles that have been fundamental to the growth of the Internet as an engine of expression and innovation.

In 2015, the FCC correctly recognized that broadband Internet access service ("BIAS") is a telecommunications service. *See In the Matter of Protecting and Promoting the Open Internet*, 30 F.C.C. Rcd. 5601 (2015) ("2015 Order"). In the Order now before the Court, the FCC has changed course to reclassify BIAS as an "information service." *In the Matter of Restoring Internet Freedom*, 33 F.C.C. Rcd. 311 (2018) ("2018 Order"). That reclassification—and the FCC's attendant decision not to prohibit BIAS providers from blocking or throttling content, or from slowing down the traffic of competitors and nonprofits to benefit companies that pay for priority treatment—is arbitrary and capricious in at least two ways.

First, the 2018 Order is based on an incorrect understanding of what BIAS necessarily includes. In order to reclassify BIAS as an information service, the Order mischaracterizes a number of functions that some BIAS providers[2] choose

[2] Because the 2018 Order governs providers of "broadband Internet access," and not other forms of access like dial-up, *amicus* uses the term "BIAS provider" to refer specifically to Internet Service Providers ("ISPs") that provide broadband access. As defined by the FCC, BIAS refers to service that offers a download speed of 25 megabits per second and an upload speed of 3 megabits per second.

to provide, such as Domain Name System ("DNS") and caching services—both by framing them as essential pieces of BIAS, and by asserting that they themselves are information services, though they are not.

Second, the 2018 Order ignores the obvious negative consequences its approach will have for online speech and innovation. As a number of *amici* previously stated to this Court, net neutrality is one of the most important free speech issues of the digital age. *See* Brief of *Amici Curiae* Electronic Frontier Foundation et al., *U.S. Telecom Ass'n. v. FCC*, No. 15-1063 (D.C. Cir. Sept. 21, 2015).

"While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace." *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017). According to Pew, nearly 90% of American adults use the Internet.[3] It has become essential to our democracy, providing real-time engagement with government,[4] a forum for anonymous criticism,[5] and a source of independent

---

See 2018 Broadband Deployment Report, FCC (Feb. 2, 2018), https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2018-broadband-deployment-report.

[3] Internet/Broadband Fact Sheet, Pew Research Center, http://www.pewinternet.org/fact-sheet/internet-broadband/ (last visited Aug. 17, 2018).

[4] *See, e.g.*, @WhiteHouse, Twitter, https://twitter.com/whitehouse; U.S. Dep't of State, Alerts and Warnings, https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html (last visited Aug. 21, 2018).

journalistic perspectives.[6] The Internet is also an important tool for innovators to test out new ideas, reach untapped markets, and build on one another's designs.[7]

BIAS providers hold the keys to this world of information. Recognizing this, and recognizing as well that net neutrality principles present from the founding of the Internet needed additional support given decreasing competition in the BIAS market, the FCC's 2015 Order crafted appropriate, enforceable rules to make sure BIAS providers would play fair. The FCC's 2018 reversal will have the opposite effect, to the serious detriment of online expression and innovation. While the 2018 Order alludes to the possibility of such harms, it offers only a market solution to them, which the evidence before the FCC showed would be inadequate.

For these reasons, the 2018 Order is arbitrary and capricious, and the Court should set it aside.

---

[5] *See* James A. Gardner, *Anonymity and Democratic Citizenship*, 19 Wm. & Mary Bill Rts. J. 927 (2011), available at http://scholarship.law.wm.edu/wmborj/vol19/iss4/6/.

[6] *See, e.g.*, Sarah Almukhtar et al., *Black Lives Upended by Policing: The Raw Videos Sparking Outrage*, N.Y. Times (last updated Aug. 21, 2018), https://www.nytimes.com/interactive/2017/08/19/us/police-videos-race.html.

[7] *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.").

ARGUMENT

I. THE RESTORING INTERNET FREEDOM ORDER IS ARBITRARY AND CAPRICIOUS BECAUSE IT MISUNDERSTANDS BIAS PROVIDERS' OFFERINGS.

The FCC's ability to regulate broadband Internet access service ("BIAS") turns in large part on whether it classifies BIAS as a "telecommunications service" or an "information service."

As amended, the Communications Act of 1934 defines a "telecommunications service" as "the offering of telecommunications," 47 U.S.C. § 153(53) (2018), which is defined in turn as "the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received," *id.* (50). In contrast, it defines an "information service" as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications." *Id.* (24).

To find that BIAS constitutes an "information service," therefore, the FCC had to determine that BIAS does more than simply transmit information chosen by the user between points chosen by the user. But BIAS does not do more; broadband Internet access service is precisely such a transmission. The 2018 Order

attempts to avoid this reality by insisting that BIAS providers "offer" various functionalities to end users that are, in fact, offered by third parties.[8]

This finding was arbitrary and capricious, violating the Administrative Procedure Act ("APA"). 5 U.S.C. § 706(2)(A). An action qualifies as arbitrary and capricious

> if the agency has . . . entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise.

Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983). "'Conclusory explanations for matters involving a central factual dispute where there is considerable evidence in conflict do not suffice to meet the deferential standards of our review.'" *Int'l Union, United Mine Workers v. Mine Safety & Health Admin.*, 626 F.3d 84, 94 (D.C. Cir. 2010). Objectively unreasonable factual conclusions, even if drawn from the record, also violate the APA. *See Allentown Mack Sales and Service, Inc. v. NLRB*, 522 U.S. 359, 374 (1998). The 2018 Order's foundational errors in understanding the BIAS offering easily qualify.

[8] *See* 2018 Order ¶¶ 30–32.

A. BIAS Providers Offer Access to Content and Services on the Internet—Not the Content and Services Themselves.

In order to find that BIAS constitutes an information service having the "capability" to engage in specific services, the FCC defines "capability" to include "ha[ving] the capacity or potential ability to be used to engage in th[os]e activities."[9] Applying this logic to phone services is instructive: it would mean that telephone companies offer pizza delivery services merely because one can use a phone to call a pizza shop that will deliver pizza. But of course telephone companies do not offer pizza delivery services.

The result is equally nonsensical when applied to BIAS, yet the FCC applies that logic to find that BIAS offerings include "social media and file sharing," "websites and online streaming and audio applications, gaming applications," and "cloud and remote servers."[10] Much like pizza shops, however, third parties—not BIAS providers—offer those services. Just like a phone service, BIAS is merely the conduit by which users can access other services.

Customers are well aware of the distinction between BIAS providers and providers of other Internet services. "It is common usage to describe what a company 'offers' to a consumer as what the consumer perceives to be the integrated finished product." *Nat'l Cable & Telecomms. Ass'n v. Brand X Internet*

[9] *Id.* ¶ 30.

[10] *Id.*

Servs., 545 U.S. 967, 990 (2005). Consumers routinely rank individual BIAS providers among the most-hated companies in America,[11] and the industry is tied for last place in customer satisfaction.[12] In contrast, consumers evaluate "edge providers" like Netflix, Google, and the thousands of small organizations and individuals operating on the Internet on their own merits. BIAS providers themselves (such as Verizon or AT&T) would no doubt be puzzled if complaints about their "offerings" included criticism of online news sources, Amazon's product review system, or Facebook's newsfeed.

B. The Domain Name System Is Not an Integral Part of a BIAS Offering.

The FCC similarly erred when it concluded that "even if 'capability' were understood as requiring more of the information processing to be performed by the classified service itself," BIAS "meets that standard" because the Domain Name System ("DNS") is "an indispensable functionality of [BIAS]."[13] On the contrary,

---

[11] Samuel Stebbins et al., *Bad Reputation: America's Top 20 Most-Hated Companies*, USA Today (Feb. 1, 2018), https://www.usatoday.com/story/money/business/2018/02/01/bad-reputation-americas-top-20-most-hated-companies/1058718001/.

[12] Aaron Pressman, *The Cable TV Industry Is Getting Even Less Popular*, Fortune (May 25, 2017), https://fortune.com/2017/05/25/cable-tv-comcast-verizon/.

[13] 2018 Order ¶¶ 33, 34.

DNS is not necessary to a BIAS offering and, in the words of the 2018 Order, BIAS providers "are not the sole providers of DNS services."[14]

DNS is essentially a phonebook for the Internet. When a person requests a website by typing the website's name (the "domain name") into a browser or by clicking a link, DNS services determine the Internet Protocol (IP) address of that domain name. Just as an individual may look to a phonebook to find the FCC's phone number, the computer of a person wishing to visit "fcc.gov" will contact a DNS server to ask for the IP address that corresponds to that domain name.

There are two types of DNS servers: "authoritative" and "resolving." Resolving servers know how to follow a chain of steps to the authoritative servers, but only authoritative servers are actually able to identify IP addresses.

Many BIAS providers, including Comcast and Viasat, do not provide authoritative DNS servers and thus do not themselves offer the functionality of authoritative DNS.[15] Rather, they provide an avenue to reach information generated elsewhere. Those that do offer authoritative DNS generally do so as an additional feature for their *enterprise web hosting* offerings, not as part of their

---

[14] *Id.* ¶ 34.

[15] *See Services | Viasat* (last visited Aug. 20, 2018), https://www.viasat.com/services (listing Viasat's services without mention on this or the click-through pages of DNS); *High Speed Internet Service from XFINITY by Comcast* (last visited Aug. 20, 2018), https://www.xfinity.com/learn/internet-service (authoritative DNS not mentioned).

BIAS offering.[16] Many BIAS providers operate resolving DNS servers, but such servers are not essential to a subscriber's Internet access. And while large numbers of BIAS subscribers use the BIAS provider's resolving servers as a conduit to reach the authoritative ones, they do so only because BIAS providers set their own servers as the default. If BIAS providers stopped operating these servers, neither service would break down; instead, BIAS providers would point users to a third-party resolving DNS server and most users would never know the difference.

As with Internet content more broadly, the FCC incorrectly attributed services offered by third parties to BIAS providers simply because they provide a conduit for reaching those services.

Just as phone users need not rely on the phone company's phonebook, Internet users can choose from a wide variety of free DNS servers operated by Google, Cisco, Cloudflare, Packet Clearing House, and others.[17] Some Internet

---

[16] *See Domain Hosting & Email Services* (last visited Aug. 20, 2018), https://www.sonic.com/business/hosting; *Domain Name System (DNS) Services – Verizon ROUTE* (last visited Aug. 20, 2018), https://www.verizondigitalmedia.com/platform/route/.

[17] Yunhong Gu, *Google Public DNS and Location-Sensitive DNS Responses*, Google Webmaster Central Blog (Dec. 15, 2014), https://webmasters.googleblog.com/2014/12/google-public-dns-and-location.html; *1.1.1.1—the Internet's Fastest, Privacy-First DNS Resolver*, Cloudflare, https://cloudflare-dns.com/; *Cloud Delivered Enterprise Security by Open DNS*, CISCO, https://www.opendns.com/; *Quad9 DNS: Internet Security and Privacy in a Few Easy Steps*, https://quad9.net/.

users even keep a local copy of a DNS database—akin to having a personal address book at the ready to avoid having to use the phone book.

Indeed, despite the strong influence of default settings, savvy users are increasingly using alternatives to BIAS providers' DNS because of pervasive "DNS hijacking," whereby BIAS providers substitute their own materials, such as advertisements, in place of error codes indicating that the requested page cannot be found. Besides being annoying, these practices create serious security vulnerabilities for subscribers.[18] The outcry in response to these practices shows that, contrary to the FCC's findings, subscribers do not expect or want BIAS providers to interject themselves into the content of information transmitted to and from DNS servers.[19]

C. Caching Is a Non-Essential and Increasingly Obsolete Practice.

Using equally faulty logic, the FCC also found that BIAS is an information service because caching is "a functionally integrated . . . component of [BIAS]."[20] However, not all BIAS providers rely on their own caching—as the 2018 Order

---

[18] *Message from the Internet Architecture Board to Stuart Lynn*, ICANN (Jan. 25, 2003), https://www.icann.org/resources/pages/iab-message-to-lynn-2003-01-25-en; Ryan Singel, *ISPs' Error Page Ads Let Hackers Hijack Entire Web, Researcher Discloses*, WIRED (Apr. 19, 2008), https://www.wired.com/2008/04/isps-error-page.

[19] *E.g.,* Evan Anderson, *Fixing Charter's DNS Hijacking*, Evan J.D. Anderson (June 23, 2010), https://ejdanderson.wordpress.com/2010/06/23/fixing-charters-dns-hijacking/.

[20] 2018 Order ¶ 41.

recognizes, but then ignores, in finding "as a factual matter [that BIAS providers] offer a single, inextricably intertwined information service" that includes caching.[21] Moreover, caching is becoming less and less useful as a result of the changing nature of the Internet.

Caching refers to the practice of a server storing a copy of data that users have requested frequently (e.g., a popular news article or a viral video), and using that copy to speed up data transmission for future requests. When the next user requests the same data, the BIAS provider's server can deliver the data from its cache, rather than sending the request all the way to and delivering the data all the way from the original source.

Internet users do not need the BIAS provider's caching to use BIAS. Some BIAS providers, such as Sonic, do not offer their own caching services at all. Without caching, requests simply travel to and from original data sources. This is the exact process, in fact, that takes place every time an Internet user requests data that isn't stored in an ISP caching server. Therefore, caching is simply a method for sending data to users more quickly, and is hardly inseparable from BIAS.

Moreover, third-party Content Delivery Networks ("CDNs") are increasingly replacing BIAS providers' caching services. The caching services of CDNs work much like those of BIAS providers, but they are operated by

[21] *Id.* ¶¶ 48, 49.

companies other than BIAS providers such as Akamai, Amazon, Cloudflare, and Microsoft, which partner with content providers. CDNs offer a distinct advantage to content providers: while BIAS caching happens automatically, CDNs allow content creators to choose exactly what data is cached and for how long. Their growing prevalence has made BIAS caching services less useful and less important.

The spread of data encryption is also making BIAS caching services increasingly obsolete. When a user requests data over an encrypted connection, the user's BIAS provider cannot see the name, location, or contents of the information requested. Thus, the BIAS provider's caching service is technologically unable to determine which resources are popular enough to cache or whether a user has requested a popular file, let alone to see the data that it would need to cache.[22]

Encryption is widely used, meaning that BIAS caching is well on its way to obsolescence. As of 2017, over half of web browsing traffic was encrypted, up from only 2% in 2010.[23] All major browsers have announced that they will only support the next version of the fundamental HTTP protocol (HTTP/2) over

[22] *See* 2018 Order ¶ 42 (noting that BIAS providers can only cache non-encrypted retrievals).

[23] Gennie Gebhart, *We're Halfway to Encrypting the Entire Web*, Electronic Frontier Foundation (Feb. 21, 2017), https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web.

encrypted connections.[24] Caching was never inextricably intertwined with Internet data transmission, and recent developments ensure that ISP caching services will become increasingly uncommon.

D. DNS and Caching Are Not Information Services.

The 2018 Order's reliance on DNS and caching to reclassify BIAS as an information service is arbitrary and capricious for the additional reason that DNS and caching are not themselves information services. Instead, they constitute user-directed transmission of information from point to point over the Internet—that is, a telecommunications service. *See* 47 U.S.C. § 153(50) and (53). Much like the specific mechanics of mail sorting and telephone routing, DNS and caching are implementation details. Those details do not change the fact that BIAS is—and is perceived to be—a service that provides end users transmission of content of their choosing between points of their choosing.

In sum, the Commission's decision to classify BIAS as an information service is based on a clear misunderstanding of the technology underlying BIAS. BIAS providers offer the transmission of information to and from the rest of the Internet. This is what Internet access means, and the FCC's attempts to characterize Internet access as something different by shoehorning supposed

[24] Dan Goodin, *New Firefox Version Says "Might as Well" to Encrypting All Web Traffic*, Ars Technica (Apr. 1, 2015), https://arstechnica.com/security/2015/04/new-firefox-version-says-might-as-well-to-encrypting-all-web-traffic/.

information services into BIAS are inconsistent with the facts of the technology and the marketplace.

II. THE 2018 ORDER IS ARBITRARY AND CAPRICIOUS BECAUSE IT FAILS TO ADDRESS THE DETRIMENTAL IMPACT ON ONLINE SPEECH AND INNOVATION.

In addition to being based on fundamental misunderstandings of what BIAS is, the reclassification described above will obstruct expression and innovation online. Finding otherwise—particularly based on the assumption that consumer choice of BIAS providers can mitigate any such effects—is objectively unreasonable.

A. Net Neutrality Was Built Into the Design of the Internet and Made the Internet Into a Powerhouse for Speech and Innovation.

When the Internet became a mass communications medium in the early 1990s, the market for Internet access was competitive. Individuals used dial-up connections, which meant connecting directly to a wide variety of Internet Service Providers ("ISPs")[25] over telephone lines. Individuals who disliked their ISP could connect to a new provider simply by dialing a different phone number. This spurred the development of a healthy and competitive ISP

[25] As noted above, "BIAS providers" refers to the subset of ISPs that provide broadband Internet access.

marketplace, with thousands of providers offering Internet access across the United States.[26]

Contrary to the FCC's finding that "the Internet as we know it developed and flourished under light-touch regulation,"[27] common carrier rules and other FCC regulations were key to fostering the Internet's early growth. These rules and regulations curbed the power of telephone companies that controlled the "last mile"— that is, the wires bringing data to individual consumers. For example, in 1975, the FCC prohibited telephone companies from blocking customers from attaching their own equipment to the phone network; this enabled the use of dial-up modems.[28] In 1980, the FCC required telephone companies to offer "data services" through separate affiliates; this prevented them from using their control of the telephone network to discriminate against unaffiliated, competing data services.[29] And, in 1983, the FCC prohibited telephone companies from charging ISPs by the minute for their customers' use of the local telephone network.

---

[26] 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 ("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.").

[27] 2018 Order ¶ 110.

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

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

This meant consumers did not have to pay per-minute fees for Internet access on top of their phone bills[30]—a practice that slowed Internet growth in Europe. The Telecommunications Act of 1996 itself began as the proposed "Antitrust Reform Act of 1992" and had the central purpose of promoting competition by banning anticompetitive practices such as excluding competitors from crucial infrastructure.[31] These common carriage regulations helped foster the emerging Internet, and are similar to the principles underlying the 2015 order that the 2018 Order overturned.

In addition to regulations, net neutrality design principles were central to the development of the Internet. The Internet consists of tens of thousands of independent networks of computers and other devices owned, operated, and maintained by different entities.[32] To facilitate global communication, each network interconnects to one or more other networks, thus the term "Internet." The networks vary widely in their architecture and underlying technology—but they are able to interconnect because they all speak the same languages ("protocols") and adhere to two basic design principles: the "network stack" and the "end-to-end principle."

---

[30] *See In the Matter of MTS and WATS Market Structure*, 97 F.C.C.2d 682 (1983).

[31] H.R. Rep. No. 102-850, at 13, 51-53 (1992).

[32] *CIDR Report for 20 Aug 18*, CIDR Report, http://www.cidr-report.org/as2.0/ (last visited Aug. 20, 2018).

The "network stack" refers to the principle that those who build applications do not need to know the implementation details of the physical networks or communication protocols that run them. Instead, each "layer" in the stack adheres to a specific set of standards.[33] This ensures that the layers of the Internet work in a standard way, rather than in a dozen idiosyncratic ways that would require programmers to know exactly what hardware or file formats will be used at every step. For example, a website operator need not know whether a user is viewing its website over fiberoptic cable or DSL, or with a Cisco router or a Netgear router. The operator simply adheres to the standards provided for its layer, and is able to interoperate with the rest of the Internet according to those common protocols.

The second key design choice was the "end-to-end" principle. This is the idea that the computers in the middle of the network should make decisions solely to efficiently and correctly route the data traveling across them. In other words,

---

[33] In the Open Systems Interconnection (OSI) model, a "layer" is defined as "a subdivision of the OSI architecture, constituted by subsystems of the same rank." *Data Networks and Open System Communications; Open Systems Interconnection—Model and Notation*, International Telecommunication Union (July 1994) at 6, https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.200-199407-I!!PDF-E&type=items. The OSI model recognizes seven layers. The Transmission Control Program (TCP) or "Internet model" recognizes five layers. *See* Vinton G. Cerf and Robert E. Kahn, *A Protocol for Packet Network Intercommunication*, IEEE (1974), https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf. Each one has its own set of standards.

they should not apply more complex rules or prioritize other goals.[34] The computers at the "ends" or the "edge" are the ones that decide how to use the information that reaches them, and meddling in the middle of the network is detrimental because it will degrade some of the uses that the endpoints might make.[35]

Critically, these principles mean that anyone can create an innovative application and count on it working, without having to negotiate with entities that operate other layers of the network stack. This flexibility was a critical reason that the modern Internet was able to develop so quickly and richly.

B. It Is Arbitrary and Capricious to Ignore the Danger the 2018 Order Poses for Speech and Innovation Online.

The 2018 Order undermines these neutral principles and structures by giving BIAS providers the power to constrain and shape expression and innovation. Because customers must go through their BIAS provider's network to reach any endpoint on the Internet (such as a website), the BIAS provider has the technological ability to downgrade or sever that link so that its subscribers cannot reach a particular endpoint, access its content, or use a particular hardware device

---

[34] B. Carpenter, *Request for Comments 2775: Internet Transparency*, "The end-to-end argument," IBM (2000), https://tools.ietf.org/html/rfc2775#section-2.1.

[35] *See* David D. Clark, *The Design Philosophy of the DARPA Internet Protocols*, ACM SIGCOMM Computer Comm. Rev., Vol. 18, No. 4, Aug. 1988, at 106; J.H. Saltzer et al., *End-to-End Arguments in System Design*, ACM Transactions on Computer Sys., Vol. 2, No. 4, Nov. 1984, at 277.

or software application to connect. By giving BIAS providers the legal power to block, throttle, or offer prioritized access to certain sources of information, the 2018 Order enables BIAS providers to make any network services—that is, services provided over a network, including everything from voice over IP to email to websites—inaccessible or less convenient to use, while making others highly appealing.

These dangers are not hypothetical. Incidents from other countries where neutrality norms have been less robust illustrate the risks. In the UK, discrimination in access affects over 75% of subscribers,[36] and the same is true for at least one in five subscribers in the European Union.[37] Chillingly, a Canadian ISP blocked union-related web sites for all of its subscribers during a labor dispute.[38] This deprived users of the ability to hear multiple sides of a political issue. Without

---

[36] 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*, p. 131 (Sept. 2013) (Published Ph.D. dissertation, University of Oxford), *available at* https://alissacooperdotcom.files.wordpress.com/2017/12/chapter6-final.pdf.

[37] Body of European Regulators for Elec. Comm., *A View of Traffic Management and Other Practices Resulting in Restrictions to the Open Internet in Europe*, pp. 8, 19-21 (May 29, 2012), *available at* http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf.

[38] *See* Ian Austen, *A Canadian Telecom's Labor Dispute Leads to Blocked Web Sites and Questions of Censorship*, N.Y. Times (Aug. 1, 2005), https://www.nytimes.com/2005/08/01/business/worldbusiness/a-canadian-telecoms-labor-dispute-leads-to-blocked.html.

network neutrality, an American BIAS provider could similarly decide to favor information from one political perspective and suppress another. Indeed, at least two large BIAS providers have censored political speech on platforms not subject to net neutrality rules: Verizon blocked pro-choice text messages[39] and AT&T censored criticism of George W. Bush during a concert webcast.[40]

In addition to threatening online expression, the 2018 Order also endangers the Internet as a space for innovation, by altering regulations that have been in place for years and by breaking the central "network stack" and "end-to-end" principles described above.

Google, for instance, started as two students with a better search algorithm. If they had needed to negotiate deals with Comcast, Verizon, and other BIAS providers, 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 eBay, Amazon, Facebook, and Twitter. They thrived in large part because BIAS providers did not have an economic veto over new applications, services, or content.

---

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

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

By contrast, breaking those principles can translate into serious security, usability, and reliability risks for end users. This destructive effect is exemplified by the recent difficulties surrounding the development of the latest version of "Transport Layer Security" ("TLS"), which acts as a wrapper of encryption around a stream of data. By the time it was being developed, various network device vendors had broken the principles by developing idiosyncratic rules for filtering "safe" and "dangerous" content. As a result, the designers and implementers of the new version of TLS had to perform months of empirical, Internet-wide surveys of filtering practices. And they had to modify the final TLS protocol in undesirable ways to work around any incompatibilities. This hampered and delayed their important work.[41]

Abandoning net neutrality protections will ignite such problems on a mass scale and will slow development of the Internet. The 2018 Order appears to recognize this danger, but the FCC has chosen merely to impose disclosure requirements on BIAS providers while abandoning the rules that would prevent the harm. [42] This does nothing to solve the problem of innovators having to

---

[41] *See, e.g.*, E-mail from Eric Rescorla to TLS mailing list (Oct. 6, 2017, 20:17 CST), available at https://mailarchive.ietf.org/arch/msg/tls/yt4otPd5u_6fOzW02TEe2e-W5G0.

[42] *See, e.g.*, 2018 Order ¶ 233 ("[I]f ISPs do not disclose key details of how they provide broadband Internet access service, that could leave entrepreneurs and small businesses participating in the Internet marketplace unable to determine how well particular existing or contemplated offerings are likely to perform for users.").

modify their products in complicated and inefficient ways to ensure compatibility with all BIAS providers, except to help them identify those idiosyncrasies that will sabotage them. On the user side, when a BIAS provider blocks a network service, it cuts off its customers from access to that service, which may have provided a better fit for the customers' needs than the services the BIAS provider permits. And it cuts off the service from access to all the potential customers who subscribe to that BIAS provider.

Indeed, a BIAS provider need not go so far as entirely blocking access to distort public discourse or the online marketplace. Throttling and paid prioritization can have similar effects because individuals respond significantly to the speed at which services load.[43]

The 2018 Order's decision to allow blocking, throttling, and prioritization (whether paid or affiliated)[44] will mean less competition and less innovation because large, entrenched businesses will be the ones that can afford to make deals with the gatekeeping BIAS providers. Other businesses and publishers unable to pay the rents sought by the BIAS providers will bear the burden of worse connectivity and a less satisfactory user experience—or none at all in the case of

[43] *See Firefox & Page Load Speed – Part II* (Apr. 5, 2010), https://blog.mozilla.org/metrics/2010/04/05/firefox-page-load-speed---part-ii/ (noting that a 2.2 second improvement in page load speed could drive 60 million additional downloads per year).

[44] *See, e.g.*, 2018 Order ¶ 220.

blocking—even if these other players have better technology or more interesting content. This will hurt competition and the marketplace of ideas alike.

Moreover, some BIAS providers offer services that compete with other services elsewhere on the Internet. Consider a BIAS provider that offers video-on-demand or phone service, for additional fees. If such a BIAS provider is allowed to block or throttle similar services from elsewhere on the Internet, it will gain a competitive advantage for its own services due strictly to its gatekeeper role, even though the other services may be technically superior.

The FCC asserts that the 2018 Order "eliminate[s] burdensome regulation that stifles innovation and deters investment" and "brighten[s] the future of innovation both within networks and at their edge."[45] This conclusion is implausible. A policy aimed at supporting sustained innovation by network services and improved internet capacity for all Americans would support clear net neutrality rules, not dismiss them.

C. It Is Arbitrary and Capricious to Conclude that Consumer Choice Can Fix these Problems.

Notwithstanding its decision to allow blocking, throttling, and prioritization, the FCC appears to recognize that such practices by BIAS providers would hurt the

[45] 2018 Order ¶¶ 1, 5.

Internet overall.[46] The FCC asserts that the Order addresses those risks by "empower[ing] Americans to choose the broadband Internet access service that best fits their needs."[47] But consumer choice cannot solve these problems.

In contrast to the competitive market of the early Internet, today a small number of companies control Internet access. Government assistance has helped incumbent BIAS providers defray the prohibitive costs of local infrastructure construction, and federal law requires phone companies to give the cable industry access to telephone poles at preferential rates set by FCC. Wireless Internet providers have also benefited from physical and regulatory groundwork laid by the radio industry, in which "existing broadcasters . . . attained their present position because of their initial government selection in competition with others before new

---

[46] *See, e.g.*, 2018 Order ¶ 117 (finding that, given that "when a broadband provider acts as a gatekeeper, it actually chokes consumer demand for the very broadband product it can supply" and that "it is therefore no surprise that many ISPs have committed to refrain from blocking or throttling lawful Internet conduct[*sic*]"); *id.* ¶ 142 (noting that "[m]any of the largest ISPs have committed in this proceeding not to block or throttle legal content," which is good for consumer protection); *id.* ¶ 170 (describing possibility that an "ISP might block or degrade edge provider traffic through arrangements for Internet traffic exchange" as a "risk"); *id.* ¶ 217 (finding that transparency rule is important because it "increases the likelihood that ISPs will abide by open Internet principles").

[47] *Id* ¶ 1; *see also id.* ¶ 153 (asserting that "market competition . . . will protect values such as free expression, to the extent that consumers value free expression as a service attribute and are aware of how their ISPs' actions affect free expression"); *id.* ¶ 265 (predicting that if any stakeholder were inclined to block or throttle, "consumer expectations, market incentives, and the deterrent threat of enforcement actions will constrain such practices *ex ante*").

technological advances opened new opportunities for further uses." *Red Lion Broad. Co. v. FCC*, 395 U.S. 367, 400 (1969). The fiberoptic BIAS market is also shaped by countless state and federal subsidies.

New competitors can offer BIAS only by building new networks from scratch. Incumbent communications companies have used this first-to-market, government-enabled advantage to establish captive customer bases for BIAS. Guarded by significant barriers to entry, the BIAS market is a monopoly or, at least, an oligopoly, in most of the country.

As the Commission's own data shows, close to one half of American households can access only one broadband provider.[48] Thus, many consumers who want broadband connectivity will have no choice but to contract with that one provider. Without net neutrality, that one provider's decisions about content will determine what (or at least how easily) all of its customers can access which information. Without net neutrality, that reality may be just as bad for the additional quarter of American households who have only two available providers,[49] as they may be forced to choose between two companies offering different plans that nevertheless both engage in blocking, throttling, or paid

[48] *See Internet Access Services: Status as of December 31, 2016*, FCC (Feb. 2018), https://docs.fcc.gov/public/attachments/DOC-349074A1.pdf, Figure 4 (showing that 43% of households have no choice for providers offering 25Mbps or more).

[49] *Id.*

prioritization. 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 interfering with their data. *See Verizon v. FCC*, 740 F.3d 623, 646-47 (D.C. Cir. 2014); *see also* 2018 Order ¶ 128 (noting but then rejecting "[t]he [FCC's] prior findings . . . [that] voluntary churn rates for broadband service [are] quite low.").

As this Court recognized in *Verizon* and reaffirmed in *U.S. Telecom*, the state of the market means that 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") (reasoning adopted by *U.S. Telecom Ass'n v. FCC*, 825 F.3d 674, 734 (D.C. Cir. 2016)).

Without the option to engage in paid prioritization, ISPs will be encouraged to build out capacity so they could then charge customers higher rates for more bandwidth. Once paid prioritization is an option, every provider's incentive is to congest the network. That way, they stand to make money from both sides: their customer base, which has no other choice, and network service providers like

Netflix and YouTube, which will pay for prioritization so that their traffic makes it through when the network is congested.[50]

Accordingly, far from enabling customers to use their market power to ensure that ISPs do not distort innovation or public discourse, the reality of today's BIAS market shows that ISPs will use their power to keep networks congested and to choose winners and losers among other Internet services and forums.

Under the APA, "an agency may not 'entirely fai[l] to consider an important aspect of the problem' when deciding whether regulation is appropriate." *Michigan v. EPA*, 135 S. Ct. 2699, 2707 (2015) (alteration in original) (quoting *Motor Veh. Mfrs. Ass'n v. State Farm Ins*, 463 U.S. 29 at 43 (1983)). In assuming that competition will cure harms to free expression and innovation, while ignoring the undisputed *lack* of competition for at least three-quarters of American households, the Commission has impermissibly done just that.

CONCLUSION

For the foregoing reasons, this Court should hold that the FCC's 2018 Order is arbitrary and capricious and set it aside.

[50] *See* Vishal Misra, *Net Neutrality Is All Good and Fine; The Real Problem Is Elsewhere* (2014), https://www.cs.columbia.edu/2014/net-neutrality/.

Dated: August 27, 2018

By: */s/ Mitchell Stoltz*

Mitchell Stoltz
Corynne McSherry
Kit Walsh
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
Attorneys for Amicus Curiae

CERTIFICATE OF COMPLIANCE

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

1. This Brief of *Amicus Curiae* Electronic Frontier Foundation in Support of Petitioners complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,407 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: August 27, 2018

By: /s/ Mitchell Stoltz

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

Counsel for Amicus Curiae

CERTIFICATE OF SERVICE

I, Mitchell Stoltz, hereby certify that on August 27, 2018, I electronically filed the foregoing Brief Amicus Curiae of Electronic Frontier Foundation with the United States Court of Appeals for the District of Columbia through the Court's CM/ECF system, which will serve all Counsel who are registered CM/ECF users.

By: */s/ Mitchell Stoltz*
Mitchell Stoltz

Attorneys for Amicus Curiae
Electronic Frontier Foundation

APPENDIX A

STATEMENT OF AGREEMENT BY DEVELOPERS OF THE INTERNET

The undersigned join and agree with the Amicus Brief of the Electronic Frontier Foundation in Support of Petitioners, to which this appendix is attached. All listed affiliations are for identification purposes only unless otherwise noted.

- Vint Cerf, Internet Pioneer
- Susan Landau, Tufts University
- John Bartas, Technical lead on the first commercial Internet software for IBM PCs
- Jonathan F. Spencer, IT Solutions Architect, United States Postal Service
- Rebecca Parsons, Chief Technology Officer, ThoughtWorks
- Brian Behlendorf, Executive Director, Hyperledger, the Linux Foundation
- Chris Lonnen, Director of Systems Engineering, Mozilla
- John Gilmore, co-founder, EFF
- Robert Oliver, Solution Architect, Dassault Systèmes
- Ben Mobley, CEO, Bad Rabbit Security Limited
- Gary Cohn, Network Engineer
- Jeremy Mill, Software Engineer, Otis Elevator
- Dr. James L. Doty, Electrical Engineer, retired
- Joshua Turton, Senior Developer, Phase2
- Aaron Rabinowitz, Network Security Engineer
- Andrew Wolfe, Term Lecturer, Santa Clara University

- Cliff Sojourner, networking and computer scientist
- Michael Meyer, Information Security Specialist, Applied Tech Solutions
- Tyler Lawrence, Founder and CEO, ArcPoint Consulting
- James Graebner, Network Engineer, Charter Communications
- AJ Bahnken, Security Engineer, Mozilla
- Adrienne Platner, Software Engineer, Thorn
- Greg Sadetsky, Technologist, 10x Management
- Randy Bush, Member Technical Staff. Arrcus Inc.
- Alexander Bryan, Data Recovery Expert. Springfield Data Recovery
- Sean O'Brien, founder of Yale Privacy Lab and Lecturer in Law at Yale Law School
- Mark Ghuneim, ex Dir Content Twitter, SVP Sony, Current CEO Mediaeater.
- Patrick Dyl, Access Transport Technician, Coz Communications
- Michael Royall, Network Engineer, Fortissimo Consulting
- Robert Berry, Software Engineer, Google
- T. Matthew Moody, Senior Web Developer, Aquent
- Gonzo Granzeau, Head of Devops for E-commerce, First Data
- George Pagel, Sr. Information Security Consultant, Wipfli LLP
- C. Lee Davis, DevOps Manager, Fabric.com
- Brett Lipschultz, Technology Auditor, Goldman Sachs

- Jonathan Brossard, Head of Security, Change.org
- Lester Earnest, Senior Research Computer Scientist Emeritus, Stanford University
- Todd Troxell, CTO, Anycoin
- Daniel Weinand, Director of Platform, Valimail
- Kevin Christopher Henry, Software Engineer
- Rita M. Johnson, IT& Broadcast Engineer
- Alfred Ganz, network infrastructure consultant (retired)
- Dr. Karen LaBonte, education technology specialist
- David Peters, Director of Engineering, Zillow Group
- Gordon Jacobson, WAN Consultant and Co-founder of The Iramp Network, Circa 1995
- Joshua Colvin, Software Engineer
- Alisa Peters, Lead Backend Software Engineer, Thrive Global
- Jonathan Major, Sr Network Engineer, Internetwork Engineering
- Mike Trest, Principal Consultant, Trest Consulting
- James Renken, Managing Member, Sandwich.Net, LLC
- John Larkin, Senior Staff Engineer, Qualcomm Inc.
- Bradley J. Greer, University of Washington, IT Chief Technology Officer
- David R. S. Robinson, Technologist, Recursive Decent Code
- Julian Macassey, Telecommunications engineer
- Chip Rosenthal, Staff Engineer, major broadband manufacturer

- Thomas Chappelow, Principal Consultant, Data Protection People
- Jonathan David Arndt, Programmer
- Prof. Barbara A. Cherry, The Media School, Indiana University
- Justin Findlay, Data Scientist, Microsoft
- George Yanos, Principal Research Programmer,
  University of Illinois at Chicago
- John Souvestre, Founder. Southern Star ISP, and Network Engineer
- Mike Harris, Owner, 556 Forensics, LLC
- Hugo Corbucci, Senior Developer, DigitalOcean
- Nolan Earl, Software Developer
- Rich Seifert (M.S.E.E., M.B.A., J.D.)
  President, Networks & Communications Consulting
- Jeffrey Nyeboer, Science Director, The Logic Progic
- Amy Sample Ward, CEO, NTEN
- Jill Rouleau, Senior Software Engineer, Red Hat
- Stefano Zanero, Chair, Cybersecurity STC, IEEE Computer Society
- Derek DePasture, Sr. Network Engineer, BluePearl Veterinary Partners
- Andrew Gallo, Principal Network Architect,
  George Washington University
- Julien Mailland, Assistant Professor, Indiana University Media School
- Ryan O'Grady, Research Scientist, Soar Technology, Inc.
- Ryanne Fox, Sr. Engineer, GoDaddy
- Matt Dunlap, Autonomous Vehicle Engineer, Optimus Ride

- Jonathan Poritz, Associate Professor of Mathematics, Colorado State University-Pueblo
- William Bierman, GrammaTech, Inc.
- Jamie Lawrence, Systems Engineer, SquareTrade
- George Roehsner, Chief Information Officer, Market USA Federal Credit Union
- Zachary Tschirhart, Research Scientist at AMD Research
- Kenneth Breeman
- Stephen Derby, Sr. Infrastructure Engineer, Suffolk
- Jeremy Schwartz, CISSP, B.S. MIS
- Tony R. Donnes, Attorney at Law, A Limited Liability Law Company
- Kevin Kilduff, Creative Technologist, Weber Shandwick
- David Newman, President, Network Test
- Serge Egelman, International Computer Science Institute / UC Berkeley
- Scott Campbell, Network Security Engineer, Energy Sciences Network
- Matt Cowger, Platform Architect, Pivotal
- Jeremy Galloway, Security Intelligence, Atlassian
- Andy Sayler, Senior Security Engineer, Twitter
- Brian Hinch, Head of Production, Tellart
- Daniel Zen, CTO, zen.digital
- W. Falcon Street, Chief Information Security Officer, FDEO
- Rich Kulawiec, senior Internet security architect, Fire on the Mountain
- Bryan Hanks, PMP, CSM, Technical Project Manager, HBJitney, LLC

- Casey Boardman, Software Engineer
- Steven McDougall, computer programmer
- Phil Cryer, Open source technologist and privacy advocate
- Yoji Watanabe, Security Engineer Intern, Tufts Technology Services
- Scott Forrest, IT Manager, Hobbs, Straus, Dean & Walker LLP
- Ryan Buehl, Director of Information Technology, GardaWorld Federal Services
- Daniel Albritton, Founder and CEO, Megaphone TV
- Mike Doherty, Site Reliability Engineer, Google
- Kelly Kane, Senior Infrastructure Engineer
- Erik Beeson, web developer, previously with VSee and Plex
- Connor Mason, Linux Engineer, Secure-24
- David Xia, infrastructure engineer, Spotify
- Jeff Harlan, Network Automation Engineer, Oath Inc.
- Eduardo Ariño de la Rubia, Data Scientist and Pillar Lead, Facebook
- Carey Smith, UX Design Technologist for Volkswagen Group of America
- Nick Sardo, Nicholas Sardo Consulting
- Lee Aber, Chief Information Security Officer, OwnBackup
- Oge Nnadi, Software Artisan, Pillar Technology
- Christopher Arnold, Security Engineer, IEEE
- Kitt Diebold, Chief Technology Officer, Managed Services Team

- Steven M. Bellovin, Percy K. and Vida L.W. Hudson Professor of Computer Science, Columbia University, Affiliate faculty, Columbia Law School
- Charlton Austin, CTO, The Tuesday Company
- Nikola Atanasovski, Information Security Consultant, n.a. Offsec
- Peter Franušić, Sargo Secure Communications
- Cory Francis Myers, consultant and technologist
- Raven Alder, Principal Engineer, Nexum, Inc.
- Roxanne Gentile, Director of Technology
- Sidney San Martín, Software Engineer, Google
- Liam Carolan, Technologist, QuantumNet Media, LLC
- John LeFevre, Information Technology Professional
- Patrick Koppula, Head of Product and Founder, GarageBand.com
- Joshua Grose, Sr. Principal Cloud & Cyber Security Engineer, SAIC
- Daniel Tsadok, Assistant Adjunct Professor, Media Arts and Technology Department, Borough of Manhattan Community College
- Justin Mack, Sr. Product Manager, Domains, MarkMonitor