Comment re: Notice of Proposed Rulemaking on
Protecting and Promoting the Open Internet

GN Docket No. 14-28

Executive Summary

Internet users in the United States are currently at risk. Internet service providers could apply intentional and arbitrary restrictions on a user's access to the open and neutral internet, imposing what we call "network discrimination," without legal repercussions. Network discrimination takes the form of:

- slowing or "throttling" internet speeds
- blocking applications, competing services, entire websites, and even users
- preferential treatment for a provider's services
- degradation of infrastructure
- increased privacy invasions

This discrimination occurs daily on networks worldwide. Such anti-competitive practices by ISPs impinge on a host of human rights, including user privacy and freedom of expression, with the same tools that many governments employ to monitor and censor traffic online. With unstable and restricted access to goods, services, and tools on the "network of networks," many internet users - including those communities whose digital rights Access defends and extends - lose the opportunity to speak out and innovate online.

Seeing the benefits of the open internet and innovation, legislators and regulators across the world are enshrining "network neutrality" into law. Based on three principles of *end to end* connections, *best effort* traffic delivery, and *innovation without permission* for anyone or any entity, net neutrality is fundamental to ensuring open and equal access to this innovative marketplace of ideas, commerce, culture, and expression.

U.S. users exercise the same human rights and deserve the same protections in order to freely access the open internet. No entity is equipped with a stronger arsenal to defend U.S. users on this issue than the Federal Communications Commission, but the Commission seeks comment on a number of standards that still enable blocking, throttling, and other discriminatory practices, misalign incentives to develop internet infrastructure, and open the door to staggering privacy violations.

The FCC must grab this opportunity to assert its full authority under Title II, and implement strong regulations protecting the open internet and innovation online. These regulations would:

- strictly define specialized services
- go beyond transparency, while increasing accountability for data and surveillance
- secure investment in the entire network's infrastructure
- bolster mobile broadband rules, setting international precedents
- limit traffic management
- scrutinize peering and interconnection upstream

Through reclassification of broadband internet access services, the FCC will apply common carriage rules to ISPs, correctly, in their role as telecommunications service providers. The Commission can then eliminate discriminatory, opaque, and invasive network management practices across mobile and fixed connections. Setting a global precedent, and securing the rights of U.S. users at risk, the FCC will protect the internet's place as a haven for expression and innovation in the 21st century.

1. Introduction

A. Who we are

Access is an international human rights organization that extends and defends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

Access appreciates this opportunity to comment on the Federal Communications Commission's Notice of Proposed Rulemaking (NPRM) on Protecting and Promoting the Open Internet. With this comment, Access will show that reclassification of broadband internet access as a telecommunications service, followed by strong net neutrality regulations, is necessary to ensure open and equal access to this innovative marketplace of ideas, commerce, culture, and expression.

B. What is net neutrality

The internet's continued success is based on three foundational principles:

First, the *end to end* principle ensures that all points in the network should be able to connect to all other points in the network. Second, the *best effort* principle guarantees that all providers of the internet should make their best effort to deliver traffic from point to point as expeditiously as possible. Finally, the *innovation without permission* principle states that everyone should be able to innovate without permission from anyone or any entity.

These principles can be collectively defined as network neutrality, which is fundamental to ensure that the internet remains an innovative marketplace of ideas, commerce, culture, and expression.

In practice, net neutrality means that all traffic on the internet is treated on an equal basis, no matter the origin, destination, type of content, or means (e.g. equipment or protocols). Any deviation from this principle, for instance for traffic management purposes, must be proportionate, temporary, targeted, transparent, and in accordance

with relevant laws and regulations. If these criteria are not respected, users then face network discrimination.

C. What is at stake: the open internet, innovation, and human rights online

Unfettered access to the internet is recognized as a basic human right.[1] Frank la Rue, UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, has underlined the fact that the internet is not only a gateway through which fundamental rights can be realized, notably the freedoms of expression and association, but also the rights to access culture and education.[2] Sir Tim Berners-Lee, inventor of the world wide web, notes that an open and neutral internet, without discriminatory interference of any sort, safeguards the fundamental rights to privacy and data protection, which are crucial for the thriving of healthy democracies.[3] In addition, technological innovations have expanded connectivity worldwide and catalyzed a thriving ecosystem of services that have become a disruptive and beneficial force in the global economy.

Access to this resource does not always come freely. Indeed, the Access global community consists of digital activists, human rights defenders, journalists, civil society groups, and other users around the world facing restrictions, retaliation, and obstacles to realization of human rights online. An open and net neutral internet allows these individuals and groups to create content, upload photos and videos, and spark viral campaigns that alert the world to threats they face. Without the voices of vulnerable communities - those who suffer disproportionately from paid prioritization - the internet ecosystem as a whole will suffer, its fundamental openness lost.

D. Why the FCC must reclassify

Despite its very public benefits, the internet remains largely a privately-owned and operated sphere. Incentives for its continued development, through digital platforms as well as physical infrastructure, depend on smart policymaking. Net neutrality regulation rights the balance of incentives on development, and ensures open and equal access to this innovative marketplace of ideas, commerce, culture, and expression. Recognizing these possibilities, legislatures in Chile, Slovenia, Mexico, the

[1] United Nations Declares Internet Access a Basic Human Right, The Atlantic, 2011: http://bit.ly/isO8oq.
[2] Report of the special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, 2011: http://bit.ly/kNHvvm.
[3] The Web Index, The Web Foundation: http://bit.ly/rhW1F2

Netherlands, Brazil, and even the entire European Union, have enshrined net neutrality into law or are on the way towards doing so.[4]

Yet, at this moment, users and networks in the U.S. are at risk of long-term harm from ISPs who - chasing incentives to maximize profits - would seek short-term gains. Without the Open Internet Order in place, and lacking any meaningful authority under Section 706 of the Telecommunications Act of 1996 to enforce meaningful anti-discrimination rules, the FCC cannot protect U.S. users from network discrimination in its many forms, like throttled networks or the slower side of paid-priority "fast lanes." By reclassifying broadband internet access under Title II's common carriage rules, the FCC will assert its proper authority to ensure that the internet remains an open and innovative platform for all.

Network neutrality regulation allows for the free flow of content, applications, and services, while increasing diversity in the types of equipment and protocols that may be used. Reclassification will help guarantee a level playing field for all web sites and emerging technologies, to the benefit of U.S. internet users, established platforms, and startups of all stripes. Following on with strong regulations, and appropriate forbearance, the FCC can protect net neutrality in the U.S. and set a clear precedent for global protection of human rights online.

2. Network discrimination at work

"Network discrimination" refers to the tendency of ISPs to intentionally and arbitrarily apply restrictions to users' access to the open and neutral internet.[5] Implemented through a wide variety of means, legal or otherwise, network discrimination adversely impacts human rights online, including the rights to privacy, freedom of expression, and access to information, and must be vigilantly regulated to ensure the internet's success as a haven of openness and innovation.

[4] *See*, e.g., https://www.accessnow.org/blog/2013/12/10/human-rights-day-network-neutrality-key-to-preserving-online-privacy (Regarding Chile, Slovenia, and the Netherlands net neutrality laws); http://thehill.com/blogs/congress-blog/technology/206137-net-neutrality-eu-brazil-and-us (Regarding Brazil, EU net neutrality laws); https://www.accessnow.org/blog/2014/04/03/the-european-parliament-takes-important-step-to-enshrine-net-neutrality-int (Regarding EU net neutrality laws); https://www.accessnow.org/blog/2014/07/09/mexico-passes-new-online-surveillance-law (Mexico).

[5] Q&A on Network discrimination in Europe, Access, 2013: http:// bit.ly/11fUriz.

Generally speaking, network discrimination can take place in the following ways:

A. Blocking of applications and services

In order to maximize profits, some ISPs - that also offer their own services and applications online - exclude certain services and applications of competing market players. For example, in 2008, the FCC condemned Comcast's practice of selectively targeting and interfering with connections of peer-to-peer applications.[6] This discriminatory and arbitrary practice threatened the benefits of an open and accessible internet. On the mobile side, before late 2009, AT&T did not allow for VoIP applications to be used with 3G data on the iPhone.[7] This stopped an innovative, cost effective, and emerging technology from directly competing with AT&T.

B. Slowing or "throttling" internet speeds

Some ISPs slow down specific services like YouTube, applications like Skype, and traffic like peer-to-peer data flows. Given the high latency (delay) sensitivity of many applications, ISPs are able to compromise the correct functioning of these services by slowing them down, thus preventing the services from running properly. Throttling of file-sharing applications like BitTorrent by ISPs is common around the world, including in the U.S., even though peer-to-peer file transfers are not illegal.[8]

C. Preferential treatment of services and platforms

Taking advantage of their dominant status in regional markets, last-mile ISPs like AT&T, Comcast, and Verizon can in effect choose winners and losers by favoring one application or service over another."[9] ISPs have also imposed data caps on internet access contracts while granting data allowance exceptions to their own proprietary streaming services.[10] In 2014, T-Mobile allowed customers to access specific streaming services without decreasing their individual data usage. Any new or developing service will remain at a disadvantage until they are included within this exception[11]; generally only large, well-established companies can afford this preferential treatment. Thus, where ISPs essentially lord over a certain market, like

---

[6] 23 FCC Rcd 13028, 13054 , 23 FCC Rcd 13028 (F.C.C. 2008)
[7] AT&T Relents, Opens iPhone to Skype, VoIP, Wired, 2009: http://www.wired.com/2009/10/iphone-att-skype
[8] Is your Internet provider throttling BitTorrent traffic? Find out, ZD Net, 2014, http://www.zdnet.com/is-your-internet-provider-throttling-bittorrent-traffic-find-out-7000025548.
[9] Of CDNs, Netflix, Net Neutrality, and Cable Fu#$@!ery., 2014, http://www.wetmachine.com/tales-of-the-sausage-factory/of-cdns-netflix-net-neutrality-and-cable-fuery/
[10] Net Neutrality - Ending Network Discrimination in Europe, Access, https://s3.amazonaws.com/access.3cdn.net/653b3b0adb37e88f4b_u7m6vw480.pdf citing to Deutsche Telekom's "anti-net- neutrality" plans alarm German government, Gigaom, 2013: http://bit.ly/17jT8QR
[11] T-Mobile's Unlimited Music Streaming Is the Worst for Net Neutrality, 2014, http://time.com/2901142/t-mobile-unlimited-music-net-neutrality/

music streaming services, its network discrimination discourages innovation and causes a lack of competition.

D. Increased risk of privacy violations

To implement traffic management, ISPs often use tools with highly invasive capacities that can execute blocking, shaping, or filtering of data for unlawful political, social, and commercial purposes. These tools include deep packet inspection (DPI) technology. DPI allows ISPs - and anyone tapped into their networks - to identify and filter content while it traverses the internet, and make a copy of the traffic.[12] DPI is the go-to mechanism governments across the world employ to invade user privacy and censor communications and content with staggering breadth and depth.[13] In 2006, AT&T and the NSA were caught using DPI-capable technology in San Francisco to sort through all traffic flowing through a major switching station, in order to pick out specific messages based on targets like an e-mail address.[14] Left unregulated, under paid priority schemes, ISPs will be incentivized to increase use of DPI to scour internet traffic in search of content to prioritize or degrade, down to the level of individual subscribers.

E. Blocking websites

In the U.S. and abroad, ISPs often block websites at their own initiative or at request of governmental authorities for a number of reasons, including to secure their network, avoid competition, enforce intellectual property rules, and for unlawful social or political purposes. For instance, U.S. legislators and officials have proposed that ISPs block access to websites to stop websites that facilitate file sharing, proposals that burden ISPs while failing to analyze its effects or even why file sharing occurs.[15] Placing companies in the position of playing judge, jury, and executioner over online content, creates a perverse incentive to censor speech. In the UK, where the government mandates blocking by ISPs, preliminary tests show that nearly 20 percent of sites - 19,000 of the 100,000 tested, a huge percentage - are blocked by one ISP or another.[16]

---

[12] Net Neutrality, http://www.edri.org/files/paper08_netneutrality.pdf
[13] http://edri.org/files/paper08_netneutrality.pdf citing to https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf at page 12
[14] The NSA Is Building the Country's Biggest Spy Center (Watch What You Say), Wired, 2012, http://www.wired.com/2012/03/ff_nsadatacenter/all/
[15] *See* White House IP Chief Talks Tough on Online Piracy, Datamation, 2010: http://www.datamation.com/secu/article.php/3905746/White-House-IP-Chief-Talks-Tough-on-Online-Piracy.htm;
[16] ORG's Blocked project finds almost 1 in 5 sites are blocked by filters, ORG, 2014, https://www.openrightsgroup.org/blog/2014/blockedproject; See Blocked, 2014, https://www.blocked.org.uk

F. Economic incentives to divest from the public good

Without regulation and balanced incentives, ISPs seeking short term profits could raise the value of paid priority options at the expense of other offerings. In practice, ISPs could invest in infrastructure to disproportionately improve the priority option, cease investment in infrastructure that helps the network as a whole, create artificial scarcity, or even degrade the quality of the current non-priority infrastructure to make prioritized options seem more attractive.[17] All of these results will create short-term profits for ISPs in exchange for long-term loss in access for users to the open internet.

Not satisfied with payments from tens of millions of ordinary subscribers, last-mile broadband access providers could also double- and triple-dip, receiving payments two or three times for providing the same service.[18] How could they do this? By asserting market power, even to the point of slowing service, to extract additional fees for the same or similar services from individual consumers, edge providers (or providers of content, applications, services, and devices on the internet), and backbone providers. In 2014, backbone peering provider Level 3 reported that, of all its global partners, large ISPs in the United States who enjoy dominant market shares were the only ISPs unwilling to expand the capacity of congested ports.[19] Further, the FCC is currently investigating why users received varied and throttled access to the popular video service Netflix[20] via ISPs that offered competing services - a scenario that merits particular scrutiny for evidence of network discrimination.

G. Reduced incentives to invest in emerging technology

A discriminatory network will reduce the economic incentive of edge providers to create new innovative products and services because of the concern that ISP permission is necessary for success. This is especially problematic when initial profits

---

[17] Choi, Jay Pil and Kim, Byung-Cheol, Net Neutrality and Investment Incentives (March 2010). RAND Journal of Economics, Vol. 41, No. 3, 2010 at 23. Available at SSRN: http://ssrn.com/abstract=1285639 at page 4, 16, 17, 22, and 32

[18] *See* Netflix Pays Verizon in Streaming Deal, Following Comcast Pact, 2014 http://time.com/80192/netflix-verizon-paid-peering-agreement/ (Verizon paid-peering agreement with Netflix); Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014) (Verizon noting they would be interested in exploring paid prioritization opportunities with edge providers); Netflix packets being dropped every day because Verizon wants more money, 2014, http://arstechnica.com/information-technology/2014/02/netflix-packets-being-dropped-every-day-because-verizon-wants-more-money/ (Verizon demanding money from Cogent before it will upgrade infrastructure to handle overwhelming demand).

[19] Observations of an Internet Middleman, Level 3, 2014, http://blog.level3.com/global-connectivity/observations-internet-middleman/ (Of 51 peering partners, 12 had congested networks. Of those 12, 6 are unwilling to make upgrades. All 6 are large broadband consumer networks with a dominant or exclusive market share. 5 are in the United States, one in Europe).

[20] The FCC is looking into Netflix's issues with Comcast and Verizon, 2014, http://www.engadget.com/2014/06/13/fcc-is-looking-into-netflixs-issues-with-comcast-and-verizon/

are low but the potential for technology improvement is huge.[21] For example, the continuing development of VoIP applications such as Skype or the development of over-the-top SMS alternatives could be affected. In these types of cases, edge provider fear of future ISP rent extraction will adversely affect the incentive to invest. Venture capitalist Brad Burnham echoed these concerns when he said, in response to these proposed rules, that his firm will "stay away from" startups working on video and media business models.[22] Net neutrality regulation would restore investment incentives for edge providers by alleviating their fear of potentially harmful ISP network discrimination.

3. Steps toward net neutrality

Confronting these many obstacles and discriminatory practices, regulators in the U.S. and abroad have often responded with smart measures in defense of the three principles underlying net neutrality. Based on several questions in the NPRM, Access has identified steps the FCC should take once it reclassifies and asserts full authority over broadband internet access services.

A. Defining specialized services

The Commission requests comments on how it can ensure that the specialized services exception is not used to circumvent the open internet rules. Specifically, "Should the Commission define 'specialized services'?" (NPRM Para. 60)

Yes, the Commission must define "specialized services." The lack of a clear definition could enable and even encourage widespread discrimination on the network, undermining the Commission's intent in the proposed rule. A broad, faulty interpretation could effectively create a two-tiered internet, where ISPs could determine which content would be delivered first, through a fast lane, at the expense of all the other online services left in a slow lane. This faulty definition would undermine the *best effort* principle, according to which all providers of the internet should deliver traffic from point to point as expeditiously as possible. It would also violate the *innovation without permission* principle, as online services might be forced to make commercial agreements with ISPs in order to access the fast lane and ISP customers. The harm to innovation and competition in the market and to the enjoyment of human rights on the internet would be severe.

---

[21] Choi, Jay Pil and Kim, Byung-Cheol, Net Neutrality and Investment Incentives (March 2010). RAND Journal of Economics, Vol. 41, No. 3, 2010 at 23. Available at SSRN: http://ssrn.com/abstract=1285639 at 27.

[22] The FCC's new net neutrality proposal is already ruining the Internet, 2014, http://bgr.com/2014/05/07/fcc-net-neutrality-proposal-ruining-internet/

Despite their threat to net neutrality, adequate regulation and a strict definition of specialized services can mitigate the risks. In order for their development to avoid harming the open internet, specialized services must meet four criteria:

1) provide an enhanced quality of service; 2) not be marketed or usable as a substitute for open internet access services; 3) not replace functionally identical online service; and 4) the network capacity used must be clearly separate from open internet access networks.

Once this definition takes hold, the FCC must follow on with active enforcement to ensure open and equal access to this innovative marketplace of ideas, commerce, culture, and expression.

B. Going beyond transparency

The Commission requests comments on its proposals for revising the transparency rules first adopted in the 2010 Open Internet Order, and upheld by the D.C. Circuit in *FCC v. Verizon*. (Paras. 63-88). Access supports the Commission's position that an efficacious transparency rule requires the disclosure of a broad range of information, and that the information must be disclosed in an accessible and comprehensible form, especially in the case of disclosures directed towards consumers. For example, users should be made aware whether connection speeds differ based on length or type of contract, device, location, or connection protocol; and whether data from certain services, types of content, or applications are count differently toward data caps and other limits.

However, we caution that transparency requirements alone do little to address network discrimination and the underlying incentives to throttle, prioritize, and obstruct traffic online. Without the ability to prevent discriminatory practices, in an environment characterized by monopoly and duopoly internet access provision, even the strongest transparency rules will not enable the FCC to defend a user's right to an unfettered internet.[23] Transparency is the first step, but definitely not the last step, to achieving net neutrality.

Transparency and accountability on surveillance

The Commission also asks for comments as to "whether there are network practices, performance characteristics, or commercial terms relating to broadband service that are particularly essential but not easily discoverable by end users absent effective

[23] *See* infra note 31; Internet Access Services: Status, 2013, https://apps.fcc.gov/edocs_public/attachmatch/DOC-324884A1.doc, at page 9 - table 5(a). See also Susan Crawford Explains the Significance of the Comcast Time Warner Cable Merger, Harvard Journal of Law and Technology, March 2014, http://jolt.law.harvard.edu/digest/telecommunications/susan-crawford-explains-the-significance-of-the-comcast-time-warner-cable-merger.

disclosure." (Para. 72) In the synopsis of its 2010 Open Internet Order, the Commission noted that effective disclosures will likely include information on policies affecting privacy, "For example, whether network management practices entail inspection of network traffic, and whether traffic information is stored, provided to third parties, or used by the carrier for non-network management purposes." (Fed. Reg. Vol. 76 No. 185 Pp. 59203-59204)

Broadband access providers, both fixed and mobile, possess an immense amount of data implicating the privacy concerns of their customers, including the content of text messages, logs of web pages visited, location history, and more. After a host of news reports have revealed the extent to which government surveillance programs and private agreements impact data held and transferred by third parties, it is essential that users know more than just whether this information is stored or provided to third parties.[24] Truly transparent disclosures of broadband provider privacy policies should also include the following information:

- What information is stored by the broadband provider, and for how long
- Policies on encryption, data security, and user notification after breach or unconsented or unlawful transfer
- Whether data from certain services, types of content, or applications are treated differently under relevant privacy policies
- All policies on geolocation data collection, transfer, and storage
- Policies on responding to law enforcement requests for stored consumer information, including for historical cell site data and "tower dumps";
- What consumer information will be turned over to law enforcement absent any court order;
- What consumer information will be turned over to law enforcement absent a warrant based on probable cause; and
- What consumer information will be turned over to law enforcement only in response to a warrant based on probable cause.

[24] *See* Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year, 2009, http://www.wired.com/2009/12/gps-data; http://www.wired.com/2011/09/cellular-customer-data/; NSA collecting phone records of millions of Verizon customers daily, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Providing this type of information, through corporate "transparency reports," is becoming a best practice for internet platforms and telecom providers.[25] By encouraging reporting on these data protection and surveillance topics, the Commission will give users another way to compare providers, and hold their ISPs - as well as government officials - accountable.

C. Protecting privacy amidst deep packet inspection

The right to privacy figures directly into regulation of net neutrality.

Under the NPRM's paid priority rules, the scale of possible privacy violations is staggering. Advanced surveillance technologies, including DPI, make it possible for ISPs to monitor the content of the internet traffic that flowing over their networks. DPI is essential to bulk surveillance, and can also be commercially exploited: DPI has been employed to track browsing habits and fuel behavioral advertising, without user consent.[26] Under "paid priority" schemes, DPI could help ISPs monitor traffic to decide which content users want, and when they want to download it.

Given its central place in network administration, and the well-documented threats it poses to user rights, DPI must be regulated. Any use of DPI should be limited to network security and management purposes (e.g., spam, malware, and cyber-attacks), or in specific cases when authorized by a court order and assessed by an independent oversight body, for a declared, necessary, and proportional purpose.

Fortunately, global precedents have shown the way to restrict DPI to increase protection of privacy. In 2012, the Netherlands became the second country in the world, after Chile, to require that internet providers limit use of DPI. Dutch legislation not only prohibits providers from throttling or filtering the connections of their customers, but also prevents DPI from being used to spy on their customers.[27] Indeed, the law specifies that network operators and service providers may only inspect or check communications per user request (and this consent may be withdrawn at any

---

[25] *See* e.g. https://www.apple.com/pr/pdf/131105reportongovinforequests3.pdf (Apple transparency report); http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html (AT&T transparency report); https://www.google.com/transparencyreport/userdatarequests/US/ (Google transparency report); http://transparency.verizon.com/ (Verizon transparency report).

[26] Andreas Kuehn & Milton Mueller, Profiling the Profilers: Deep Packet Inspection and Behavioral Advertising in Europe and the United States, Syracuse University - School of Information Studies, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2014181. See also Telegraph, BT and Phorm: how an online privacy scandal unfolded, 2011, http://www.telegraph.co.uk/technology/news/8438461/BT-and-Phorm-how-an-online-privacy-scandal-unfolded.html.

[27] Net Neutrality - Ending Network Discrimination in Europe, https://s3.amazonaws.com/access.3cdn.net/653b3b0adb37e88f4b_u7m6vw480.pdf citing to Summary from Bits of Freedom of the amended Dutch Telecommunications Act: http://bit.ly/jzE63v.

time) or insofar as network management purposes or legal orders prescribe.[28] Furthermore, the Dutch telecommunications watchdog inspects providers to ensure compliance. This landmark Dutch law should be used as a starting point for potential regulations prohibiting network discrimination in the U.S.

D. Securing infrastructure investment

Not just a series of tubes, the internet's infrastructure grows in tandem with growing demand for platforms and services online.

The "virtuous circle" framework asserts that by guaranteeing the openness of the internet and the *innovation without permission* principle, the number of attractive internet-based services and applications will continue increasing.[29] The demand for faster and better access to the internet will grow, generating more value for and a stronger incentive to invest in enhanced network capacity.[30] For their part, many investors have clearly expressed their interest in strong network neutrality rules. Open internet policies "help drive the economy, encourage innovation and reward investors," one group of investors and venture capitalists recently commented to the FCC.[31]

However, ISPs have claimed that net neutrality regulation discourages investment, saying "free riders" congest networks without paying extra.[32] But ISPs are willfully ignoring what users really pay for - they "don't buy fat pipes, they buy applications and content that require fat pipes."[33] The more happy subscribers they serve, the more providers profit from their investment in networks, and the more investors back new applications and services. In fact, a paid priority scheme upsets the balance of incentives on infrastructure investment. If ISPs were to invest in higher capacity for their "slow lanes," they would lower the relative value of their priority option.[34] Thus, regulation appears to boost the incentive for the ISP to increase overall capacity by

---

[28] https://s3.amazonaws.com/access.3cdn.net/62a6294b6db705f68c_gcm6iynrv.pdf citing to Artikel 11.2a, https://zoek.officielebekendmakingen.nl/kst-119245.html.
[29] *See* The Importance of (Real) Net Neutrality for Investment, https://s3.amazonaws.com/access.3cdn.net/fb7263bc7a41434b1c_ktm6bnw0b.pdf; The Open Internet - A platform for Growth, Plum, 2011: downloads.bbc.co.uk/aboutthebbc/insidethebbc/howwework/reports/pdf/plumbriefing_oct2011.pdf
[30] The Importance of (Real) Net Neutrality Investment, https://s3.amazonaws.com/access.3cdn.net/fb7263bc7a41434b1c_ktm6bnw0b.pdf
[31] Investors Urge FCC to Adopt Net Neutrality Rules, Reclassify Broadband Internet under Title II ,Open Mic, 2014, http://openmic.org/node/331
[32] Mohammed, Arshad (February 2007). "Verizon Executive Calls for End to Google's 'Free Lunch'", http://www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020601624.html
[33] Commissioner Robert. M. McDowell, Address to the Broadband Policy Summit III, Arlington, VA, at 13-14 (June 7, 2007) available at http://www.netcompetition.org/BB_Policy_Summit.pdf.

[34] Choi, Jay Pil and Kim, Byung-Cheol, Net Neutrality and Investment Incentives (March 2010). RAND Journal of Economics, Vol. 41, No. 3, 2010 at 23. Available at SSRN: http://ssrn.com/abstract=1285639

alleviating the need to make the first priority option more appealing. In other words, it's usually better to repave the whole road than a single lane.

Many critics of net neutrality legislation opine regulation is not necessary because customers can "vote with their feet" and switch to another provider. Unfortunately, the market available to end-users in the U.S. is far closer to a monopoly or duopoly than one characterized by robust competition. Over 65% of households only have access to *at most* one or two connections with 6 megabits per second (Mbps) downstream and at least 1.5 Mbps upstream.[35] Most of us have about as many options for home garbage pick-up as broadband providers.

E. Combating discrimination

In practice, net neutrality means that all traffic on the internet is treated on an equal basis, no matter the origin, destination, type of content, or means used to send, deliver, and receive the traffic (e.g. equipment or protocols). In the absence of anti-discrimination authority, the NPRM contains several proposed standards for its minimum blocking rule:

- The proposed Best Effort standard would require ISPs to use their best effort to deliver the "typical" level of service for each type of traffic. Yet the inherent ambiguity in defining what is "typical" leaves large room for ISPs to abuse this standard, and renders enforcement a herculean task.
- The Reasonable Person standard proposes satisfying the reasonable expectations of a typical end user. What is reasonable for one user very likely will not be what is reasonable for other users. This ambiguity will make it near impossible to enforce this standard equitably and with respect for individual rights.
- The Minimum Quantitative Performance standard proposes using technical parameters to define what is expected of ISPs. While this may draw a clear line today, it is very unclear how these expectations will evolve along with technology tomorrow. This quantitative standard will also allow ISPs wide discretion to shape future standards based on what they choose to invest in today.

As all these standards will tacitly permit discrimination online, ISPs will still be allowed some level of blocking or throttling of content, even to unusable levels. None of the proposed standards are sufficient to address ISP tomfoolery.

[35] Internet Access Services: Status, 2013, https://apps.fcc.gov/edocs_public/attachmatch/DOC-324884A1.doc at page 9 - table 5(a).

Given their novelty and vagueness, the standards will also be difficult to enforce. Battles will be fought over definitions and implementation. Small and medium-sized businesses, non-profits (like Access), and other vulnerable groups online do not have sufficient resources to confront the teams of lawyers ISPs permanently retain in Washington, D.C. These relatively small players should not carry the burden of proving discrimination under such vague provisions.

For their part, users too will be left bereft of options to uncover and stop malfeasance. If an ISP's service does not meet a user's expectations, the subscriber can do little to verify the source of the service deficiencies. Is your streaming video choppy because of the last mile ISP, the edge provider, or the backbone provider? The user would have to undertake the onerous task of switching network providers instead of simply trying a different website or running a network diagnostic test. This switching pains are amplified by high costs, long term agreements between consumers and ISPs, high upfront device installation fees, and the activation fee when changing your service provider.[36]

Due to these practical barriers, and the principled failures of the proposed standards, Access insists the Commission forego these lesser measures and reclassify broadband internet access under Title II. Only implementing a strict anti-discrimination provision will protect users at risk.

F. Catching up with mobile broadband

Since the Commission first contemplated net neutrality principles for broadband internet in the early 2000s, the broadband landscape has been altered in significant ways - notably with the development and widespread deployment of mobile broadband access. Simply put, the market for mobile applications, devices, and platforms has matured. The walls between wired and wireless gadgets and connections are crumbling.

Wireless broadband is getting more popular, and essential. The Pew Research Center's *Cell Internet Use 2013* report noted that 91% of Americans own cell phones, and 21% of mobile phone owners *mostly* access the internet using their phone.[37] This latter category, a growing group, encompasses users at risk, as the Commission itself

[36] The Cost of Connectivity, New America Foundation, 2013: http://oti.newamerica.net/publications/policy/the_cost_of_connectivity_2013
[37] Cell Internet Use 2013, PewResearchCenter, http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_CellInternetUse2013.pdf

observes in Footnote 228 of the NPRM: Americans who mostly access the internet using their mobile devices are typically the young, the less affluent, the less educated, and people of color.

The Commission asks for comments on its limited no-blocking rule for mobile broadband, adopted in 2010, specifically whether "to expand the rule's scope to include reasonable access to all applications that compete with the mobile broadband internet access provider's other services, not just those that compete with voice or video telephony services… ." (Para. 106) Access insists that, given the maturation of mobile broadband since 2010, the Commission should adopt the most comprehensive anti-blocking rule possible. In particular, a mobile broadband Internet access service shall not block consumers from accessing websites, subject to reasonable network management; nor shall such person block applications, subject to reasonable network management.[38] This discrimination distorts competition and interferes with users' ability to use the application or services of their choice. For this reason, practices such as blocking should be clearly prohibited in the rule in order to increase incentives to innovate, support *end to end* connectivity, and empower users to decide what services they want to access.

Given the growing population of Americans who rely on mobile broadband as their primary, or sole, method of accessing the internet, including those in vulnerable and marginalized communities, the Commission must act to protect their rights to access all benefits of the internet, *end-to-end*. The Commission's proposed rule is simply not enough to protect users at risk.

International precedents

The world is going mobile. Developing countries account for over half of the 2.1 billion mobile broadband subscriptions globally; many citizens in developing countries are getting their first experience of the internet through mobile devices.[39] However, these new users often encounter a restricted internet without *end to end* connectivity to sites and services. For example, applications such as YouTube, Facebook, and

[38] Reasonable Network Management is defined and discussed in section 3.G: Limiting Traffic Management of this paper.
[39] The State of Broadband 2013: Universalizing Broadband, http://www.broadbandcommission.org/Documents/bb-annualreport2013.pdf at pg. 16.

Twitter have been subject to country-wide bans in Turkey,[40] Egypt,[41] Iran,[42][43] Pakistan,[44] Syria,[45] and Thailand,[46] among others.

A weak anti-blocking rule in the U.S. will be seen and likely adapted by regulators worldwide to approve censorship practices that threaten human rights and innovation. Indeed, the U.S. approach to regulation of digital issues often serves as a point of reference. For example, international discussions and practices have converged around intellectual property treatment under the Digital Millennium Copyright Act (DMCA)[47]; recently, Mexico's Congress recently approved net neutrality provisions similar to the FCC's 2010 Open Internet Order.[48] More governments are likely considering whether to implement net neutrality legislation, and will no doubt look to the U.S. as a model.

While U.S. law and regulation will not keep foreign countries from interfering with their citizens' internet use, taking a strong position on mobile anti-blocking rules would place the U.S. in a position of leadership on an important issue of free expression, well into the future.

G. Limiting traffic management

The Commission requests comments on the use of traffic management measures by ISPs for commercial purposes. Specifically, "to what extent and in what ways do broadband providers use such tools to manage traffic, such as by excluding certain content from such an end user data cap? Might these tools be used to exploit market power or reduce competition?" (Para. 45)

---

[40] Twitter website 'blocked' in Turkey, 2014, http://www.bbc.com/news/world-europe-26677134
[41] https://twitter.com/twittercomms/status/30377205695647744
[42] Censorship fears rise as Iran blocks access to top websites, 2006, http://www.theguardian.com/technology/2006/dec/04/news.iran
[43] Iran Blocks Facebook, Twitter Sites before Elections (Update1), 2009, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=anh.uW3qNZp4
[44] YouTube blocked in Pakistan, 2012, http://www.washingtonpost.com/business/economy/youtube-blocked-in-pakistan/2012/09/17/30081fa2-00ea-11e2-b257-e1c2b3548a4a_story.html
[45] Syria goes mostly offline as protests intensify, 2011, http://opennet.net/blog/2011/06/syria-goes-mostly-offline-protests-intensify
[46] 2007: YouTube blocked in Thailand, 2007, http://www.2bangkok.com/blockedyoutube.shtml
[47] International Copyright Treaties and digital works, http://blaynehaggart.files.wordpress.com/2011/08/haggart-international-copyright-treaties-and-digital-works-implementation-issues-in-canada-and-mexico.pdf
[48] Mexico Passes New Online Surveillance Law https://www.accessnow.org/blog/2014/07/09/mexico-passes-new-online-surveillance-law

Traffic management interferes in the normal flow of internet traffic to prioritize, slow down, or block certain data, and has great potential for misuse and exploitation for anti-competitive and even unlawful ends.

While we agree that ISPs should be able to manage their networks, traffic management should only be allowed for narrowly tailored deviations from the rule, and should not include arbitrary or permanent restrictions by ISPs, as these practices go clearly against the *end-to-end* and *best effort* principles that are fundamental to the internet's functioning. For that aim, traffic management should not be employed to the detriment of competing services, or commercially motivated to the unfair advantage of access providers' own services or their business partners.

Traffic management techniques are "reasonable" when deployed for the purpose of technical maintenance of the network, namely to block spam, viruses, or denial of service attacks, or to minimize the effects of congestion, whereby equal types of traffic should be treated equally. Techniques should only be used on a temporary basis, during exceptional moments, and their impact must be necessary, proportionate and targeted to solve the particular problem. Finally, traffic management policies should have transparent and comprehensible disclosure for users and be used in accordance with the law.

H. Scrutinizing peering and interconnection

Rather than limiting itself to what comes out of the tap, the Commission should also monitor the upstream flows of data for evidence of blocking and discrimination. The Commission has requested comment on whether it should continue to *exclude* network interconnection arrangements from the purview of its rules. (Para. 59) It should not.

Network interconnection or traffic exchange arrangements come in many forms, including paid and unpaid peering, content delivery networks (CDNs), other forms of inter-network transmission of data, and provider-owned facilities that are dedicated solely to such interconnection. It's true that the operators making these agreements are often not household names, while net neutrality is fundamentally about broadband providers who effectively operate terminal monopolies. But to be effective, the proposed rules cannot simply focus on the last mile, ignoring decisions made upstream that affect the bulk of traffic and can cause latency, discriminate against edge providers, and degrade infrastructure.

In its rules, the Commission should take care not to diminish investment and deployment of infrastructure, such as provider side provisioning arrangements like

CDNs that house data closer to the end user and deliver it all through faster pipes. Rather, the FCC should focus on those arrangements where ISPs are only attempting to double or triple payments for providing the same service. The former is beneficial to the health of the network and catalyzes expression and access to information; the latter is a drag on innovation and a violation of human rights.

The Commission should at a minimum apply stringent transparency rules to these provisioning arrangements, by requiring that any contract governing interconnection or exchange of traffic between networks or providers be made public. While the Commission has already begun requesting the details of such agreements on an individual basis, a default rule requiring disclosure not just to the Commission, but publicly, should be incorporated into any order adopted by the Commission.[49]

Beyond transparency, the Commission should scrutinize these agreements, with public consultation, for their potential to facilitate network discrimination and harm user rights further downstream. To minimize concerns over exposure of proposed business deals, the FCC should adopt best practices for protecting confidential information, while developing standards that maximize public interaction and yield speedy and fair determinations regarding discriminatory agreements.

Consumers have a right to know how upstream agreements are affecting the services they pay for and the information they can access. By adopting disclosure and scrutiny of interconnection agreements in its rules, the Commission would ensure that users and edge providers have adequate knowledge and control over the interconnection marketplace.

4. Reclassify broadband internet access as a telecommunications service

Of the regulatory authorities available to the FCC, only Title II of the Telecommunications Act of 1996 provides the necessary authority for the Commission to enact net neutrality, while avoiding an exercise in regulatory needle-threading.

Reclassification of broadband internet access service as a telecommunications service is necessary to safeguard the values that enabled the internet to become a global force for expression and innovation. Reclassifying is also a proportionate

[49] FCC gets Comcast, Verizon to reveal Netflix's paid peering deals, 2014, http://arstechnica.com/tech-policy/2014/06/fcc-gets-comcast-verizon-to-reveal-netflixs-paid-peering-deals/

response to the types of discrimination and blocking that ISPs have implemented in the U.S. and abroad.

Common carrier rules should apply to ISPs. Since the 2002 classification, ISPs have crystallized in their role as providers of internet access, rather than information services like email. One of the largest ISPs, Verizon, has already tacitly acknowledged and is benefiting from aspects of common carrier status. This year, Verizon renewed one of its many FiOS cable TV franchise agreements under Title II authority of the Communications Act.[50] Here, Title II grants Verizon the benefit of using the utility-based public-rights-of-way, and of raising customer rates to fund FiOS deployment.[51] Yet, a letter Verizon signed in 2014 warns the FCC that Title II reclassification will stop broadband network investment and slow development.[52] This position seems to ignore the benefits for infrastructure investment that Verizon itself currently enjoys. Thus, the ISP appears to seek common carriage protection only where profitable. The Access community of users see through this facade, and demand across-the-board common carriage rules be applied to ISPs.

Using Title II authority is a superior option to other authorities. First, Title II has a successful track record in the wireless sphere. In 2007, the FCC employed Title II authority for voice and text roaming regulation.[53] Since implemented, the regulation has worked effectively and efficiently while wireless service has thrived.[54] Second, Section 706 authority will not allow the FCC to impose a comprehensive anti-discrimination regulation. In *Verizon v. FCC,* the court ruled that common carriers, and only common carriers, were subject to the regulation at issue.[55] The only way the Commission may lawfully exercise the authority necessary to impose the anti-discrimination regulation at the core of net neutrality is by categorizing broadband internet access service as a telecommunications service subject to common carrier regulation.

Reclassifying will save net neutrality by encouraging innovation without permission from any entity or person, incentivizing the continual investment in infrastructure to provide

---

[50] *See* http://www.verizon.com/about/community/nj_swf_renewal.htm; http://www.huffingtonpost.com/bruce-kushnick/net-neutrality-solved-ver_b_5390789.html (In 2007, Verizon had Franchises in 835 different locations in 12 states).
[51] Net Neutrality Solved: Verizon's FiOS Rides over a Title II, Common Carriage, FTTP (Fiber-to-the-Premises) Telecommunications Network, 2014, http://www.huffingtonpost.com/bruce-kushnick/net-neutrality-solved-ver_b_5390789.html
[52] http://www.broadbandforamerica.com/sites/default/files/CEOLettertoFCC-5.13.14.pdf (letter to FCC chairman from ISP heads)
[53] 47 C.F.R. § 20.12
[54] *See* Reexamination of Roaming Obligations of Commercial Mobile Radio Service Providers, WT Docket No. 05 - 265, Order on Reconsideration and Second Further Notice of Proposed Rulemaking, 25 FCC Rcd 4181 (2010).
[55] Verizon v. FCC, 740 F.3d 623, 650 (D.C. Cir. 2014).

best effort access, and reducing pressure on ISPs to monitor and monetize traffic flows in ways violating user privacy. Importantly, it will allow the internet to remain a platform for the enjoyment of human rights, where anyone can connect to any point on the global network in pursuit of information, association, commerce, expression, and more.

5. Conclusion

The United States has long been an international standard-setter on policy issues concerning human rights, and network neutrality should be no exception. Strong regulation will not only provide U.S. users with the right to receive and impart information and access an unfettered internet, free from discrimination, but would also set an important standard for the preservation and promotion of the open and neutral internet around the world. To realize and protect the full potential of the internet to enable and promote the flourishing of human rights, the FCC should reclassify broadband internet access as a common carrier by asserting its full authority over internet access services, and implementing strong and comprehensive net neutrality regulations.

***

Access is an international organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

For more information, please visit www.accessnow.org and contact:

Peter Micek
Senior Policy Counsel
peter@accessnow.org
+1-888-414-0100 x709