

---

# **Access Now Comment**

---

**FCC Notice of Proposed Rulemaking:  
Proceeding 17-108**

July 17 2017



## **Acknowledgement**

Access Now thanks Policy Fellow Alyse Rankin for her contribution to this Comment.

## **Comment supported by:**

epicenter.works (Austria)

La Quadrature du Net (France)

Electronic Frontier Norway

IT-POL Denmark

Digitalcourage (Germany)

European Digital Rights (EDRi)

# Table of Contents

<b>Executive Summary</b>	<b>3</b>
<b>1. Introduction</b>	<b>5</b>
A. Who we are	5
B. What is net neutrality?	5
C. What is at stake: The open internet, innovation, and human rights online	6
D. Why the FCC must maintain the Title II classification	8
i. Analysis: Difference between telecom services and internet applications	10
<b>2. Network discrimination at work</b>	<b>12</b>
A. Internet Conduct Standard	12
i. Zero rating and threats to the open internet	13
B. No Blocking Rule	15
C. No Throttling Rule	16
D. No Paid Prioritization Rule	16
E. Transparency Rule	19
F. Additional considerations regarding the Open Internet Rules	21
<b>3. Harms resulting from classification of BIAS as an Information Service</b>	<b>22</b>
A. Economic incentives to divest from the public good	22
B. Reduced incentives to invest in emerging technology	23
C. Uncertain grounds for infrastructure investment	25
D. More opaque peering and interconnection	27
E. Obstacles to mobile broadband access and equity	27
<b>4. Effects on regulatory structures created by the Title II Order</b>	<b>29</b>
A. Risks to the fundamental right to privacy	30
<b>5. Conclusion</b>	<b>31</b>

## Executive Summary

The reclassification of broadband internet access service as a Title I “Information Service” puts internet users in the United States at greater risk of human rights violations, and sets a poor precedent for the rights of internet users everywhere. Reclassification would allow internet service providers to apply arbitrary and egregious restrictions on people’s access to the open internet, imposing what we call “network discrimination,” without legal recourse or regulatory oversight.

Network discrimination takes the form of:

- slowing or “throttling” internet speeds
- blocking applications, competing services, websites, and users
- preferential treatment for a provider’s services or specific apps or content
- degradation of infrastructure and less affordable services
- increased capacity and incentive to invade privacy and censor content.

This discrimination occurs daily on networks worldwide. Such anti-competitive practices by ISPs directly interfere with a host of human rights, including freedom of expression and access to information. With unstable and restricted access to sites and services online, many internet users – including those communities whose digital rights Access Now defends and extends – lose the opportunity to speak out and innovate online.

Network discrimination occurs using the same tools that many governments employ to monitor and censor traffic online. Absent regulation, market incentives encourage ISPs to analyze traffic flows to maximize profits users at the expense of open, secure, and affordable data flows. This profiling and discrimination interferes with our rights to privacy and data protection.

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 efforts traffic delivery, and innovation without permission for anyone or any entity, net neutrality is fundamental to ensuring open, secure, and affordable access to this innovative marketplace of ideas, commerce, culture, and expression.

As elsewhere, people in the U.S. exercise their human rights online and deserve the same strong protections in order to freely access the open internet. No entity is equipped with a stronger arsenal to defend U.S. users than the Federal Communications Commission.

The 2015 classification of ISPs as telecommunications service providers has deterred unreasonable discrimination 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’s 2015 Title II Order protected the internet’s place as a haven for expression and innovation in the 21st century. Not just good policy, the 2015 reclassification fits best the

definitions in the 1996 Telecommunications Act. The Title II Order recognizes that people direct their ISPs to transmit information to various points on the internet, including the servers of websites. To read into the Act a geographical component, where users must know and intend to send traffic to specific physical addresses, defies logic as well as the Commission's own rulings. For example, the FCC maintains Title II classification of cellular telephony, whose users cannot be expected to direct their calls and texts to specific cell towers. Rather, the user knows the individual or entity understood to sit at the other end, and employs the provider to route traffic there. This is the role of ISPs: enabling us to connect and transmit our data without interference, as quickly and robustly as possible.

One area of new technology where threats of network discrimination proliferate is 5G. Named for the 5th generation of mobile networks, 5G would bring much-needed increases in internet speed and coverage for people across the global wireless system. The principles on which net neutrality is based, including innovation without a need to obtain permission, end-to-end connectivity, transparency, and nondiscrimination, are essential for preserving openness and competition amidst emerging standards like 5G. The FCC's powers under Title II can help ensure that the number of innovative internet-based services and applications will continue to increase. With global demand for faster and better access to the internet on the rise, internet access providers will continue to have a strong incentive to develop and invest in enhanced network capacity for all people – and things. This so-called “virtuous circle” illustrates the long-term economic benefit for telecommunications companies to invest in an open and free infrastructure.

After civil society, the private sector, and the FCC spent years of effort in regulatory, judicial, and public opinion battles to classify broadband internet access under Title II, we see no compelling or rational reason to suddenly change course and reclassify broadband under the weaker Title I. To prevent serious harm to human rights and the internet economy, in the U.S. and beyond, the FCC must maintain Title II classification.

# 1. Introduction

## A. Who we are

Access Now 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 Now's policy team works at the intersection of human rights and technology, furthering Access Now's mission by developing and promoting rights-respecting practices and policies. With staff placed strategically around the world, we seek to advance laws and global norms to affect long-term systemic change in the area of digital rights and online security, developing insightful, rights-based, and well-researched policy guidance to governments, corporations, and civil society.

Access Now appreciates this opportunity to comment on the Federal Communications Commission's Notice of Proposed Rulemaking (NPRM) on Restoring Internet Freedom. Access Now supports the work of the Federal Communications Commission (FCC) and was cited frequently in the FCC's 2015 Title II Order. With this comment, we will show that the continued classification of broadband internet access as a telecommunications service, and strong enforcement of net neutrality regulations, are necessary to ensure open, secure, and affordable access to this innovative marketplace of ideas, culture, and expression.

**These comments are supported by the following European non-for profit organisations: epicenter.works (Austria), La Quadrature du Net (France), Electronic Frontier Norway, IT-POL Denmark, Digitalcourage (Germany) and European Digital Rights (EDRi). Both EDRi and Access Now provided extensive comments<sup>1</sup> to the 2014 FCC NPRM, which led to the adoption of the FCC's 2015 Title II Order.<sup>2</sup>**

## 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 efforts principle guarantees that all providers of the internet should make their best effort to deliver traffic from point to point as expeditiously as

---

<sup>1</sup> Access Now, "Comment re: Notice of Proposed Rulemaking on Protecting and Promoting the Open Internet," 2014, <https://www.accessnow.org/cms/assets/uploads/archive/docs/NPRMFinal.pdf> See also, Access Now, "Access tells the FCC to use its authority to reclassify broadband and protect net neutrality," 18 July 2014:

<https://www.accessnow.org/access-tells-the-fcc-to-use-its-authority-to-reclassify-broadband-and-prote/>

<sup>2</sup> See EDRi's response to the 2014 FCC consultation at: <https://edri.org/edri-fcc-consultation-net-neutrality>

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, culture, and expression.

As the Global Network Neutrality Coalition states, “net neutrality requires that the internet be maintained as an open platform, on which network providers treat all content, applications and services equally, without discrimination.”<sup>3</sup> In practice, net neutrality prevents against network discrimination based on the origin, destination, type of content, or means (e.g. equipment or protocols) of transmission. 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

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. In addition to ensuring trust in digital economies, these rights are crucial for the thriving of healthy democracies.<sup>4</sup>

Unfettered access to the internet is recognized as essential to realizing our a basic human rights in the digital age. Frank la Rue,<sup>5</sup> the former UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 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.<sup>6</sup> The UN Special Rapporteur on freedom of expression is the highest independent expert on the rights to expression, opinion, and access to information in the UN system. David Kaye, the current Special Rapporteur, hailed the 2015 rules as a “real victory for freedom of expression and access to information in the United States.” He wrote, “I hope the new rules may serve as a model for other governments seeking to protect or expand an open and secure Internet.”<sup>7</sup>

---

<sup>3</sup> Global Net Neutrality Coalition, “This Is Net Neutrality”: <https://thisisnetneutrality.org>

<sup>4</sup> The World Wide Web Foundation, “The Web Index”: <http://thewebindex.org/>

<sup>5</sup> Frank La Rue, “Report of the special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,” 2011: [http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27\\_en.pdf](http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf)

<sup>6</sup> Nicholas Jackson, The Atlantic, “United Nations Declares Internet Access a Basic Human Right,” 2011: <https://theatlantic.com/technology/archive/2011/06/united-nations-declares-internet-access-a-basic-human-right/239911/>

<sup>7</sup> United Nations Human Rights Office of the High Commissioner, “A real victory for freedom of expression – UN rights expert hails US move to keep Internet open,” 2015: <http://ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15622&LangID=E>

In his 2017 report, Special Rapporteur Kaye expanded on the link between network neutrality regulation and the human right to freedom of expression.

In the digital age, the freedom to choose among information sources is meaningful only when Internet content and applications of all kinds are transmitted without undue discrimination or interference by non-State actors, including providers. The State's positive duty to promote freedom of expression argues strongly for network neutrality in order to promote the widest possible non-discriminatory access to information.<sup>8</sup>

Indeed, recognizing its importance, legislatures and regulators in 47 countries, including Chile, Slovenia, Mexico, the Netherlands, Brazil, the European Union, Iceland, and India have enshrined net neutrality into law or are on the way towards doing so.<sup>9</sup>

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. Internet access should not be taken for granted. The Access Now global community consists of digital rights 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.

---

<sup>8</sup> David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," 2015:

[http://ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32\\_AEV.doc](http://ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc)

<sup>9</sup> See, e.g.: Global Net Neutrality Coalition, <https://www.thisisnetneutrality.org>

(Regarding Chile, Slovenia, and the Netherlands net neutrality laws);

Estelle Massé, Access Now, "Human Rights Day: Network neutrality key to preserving online privacy," 2015:

<https://accessnow.org/blog/2013/12/10/human-rights-day-network-neutrality-key-to-preserving-online-privacy>

(Regarding Brazil, EU net neutrality laws);

Danielle Kehl, The Hill, "US should look to Brazil and the EU for strong net neutrality rules," 2014:

<http://thehill.com/blogs/congress-blog/technology/206137-net-neutrality-eu-brazil-and-us>

(Regarding EU net neutrality laws);

Estelle Massé, Access Now, "The European Parliament takes important step to enshrine net neutrality into law", 2014:

<https://accessnow.org/blog/2014/04/03/the-european-parliament-takes-important-step-to-enshrine-net-neutrality-int>

(Regarding Mexico net neutrality laws)

Peter Micek, Access Now, "Mexico passes new online surveillance law," 2014:

<https://accessnow.org/blog/2014/07/09/mexico-passes-new-online-surveillance-law>;

<https://www.accessnow.org/iceland-path-net-neutrality/> (Regarding Icelandic law);

<https://www.accessnow.org/indian-regulator-stands-up-for-net-neutrality-rules-against-zero-rated-services/> (Regarding India's net neutrality regulation).



## D. Why the FCC must maintain the Title II classification

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 that protects the public interest. Net neutrality regulation rights the balance of incentives for the internet's growth, and helps ensure open, secure, and affordable access.

According to the 2015 Title II Order, the FCC's own findings show that, "broadband providers have the incentive and ability to discriminate in their handling of network traffic in ways that can harm the virtuous cycle of innovation, increased end-user demand for broadband access, and increased investment in broadband network infrastructure technologies."<sup>10</sup>

We agree. Reclassifying broadband internet access service under Title I information puts U.S. broadband users at risk of long-term harm from ISPs seeking short term gains. Without the Title II 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." Title II classification of broadband internet access services ensures that the FCC can assert its proper authority to ensure that the internet remains an open and innovative platform for all.

More broadly, common carrier rules should apply to ISPs. Since the 2002 classification, ISPs have crystallized in their role as providers of internet access, enabling users to navigate between endpoints, rather than providing information services like email. One of the largest ISPs, Verizon, has already tacitly acknowledged and is benefiting from aspects of common carrier status, and operated for years utilizing "title shopping," providing a Title II service with a Title I classification. In 2015, Verizon renewed one of its many FiOS cable TV franchise agreements under Title II authority of the Communications Act.<sup>11</sup> Here, Title II granted Verizon the benefit of using the utility-based public-rights-of-way, and of raising customer rates to fund FiOS deployment.<sup>12</sup> Yet, a letter Verizon signed in 2014 warned the FCC that Title II

---

<sup>10</sup> Federal Communications Commission, "Title II Order" at para. 136, 2015:

<sup>11</sup> See e.g.: Bruce Kushnick, Huffington Post, "'Title Shopping' Exposed: Verizon's FiOS is Based on a Title II, FTTP Network. Shame They Never Told the Court, the FCC or the Public," 2014:

[http://huffingtonpost.com/bruce-kushnick/title-shopping-exposed-ve\\_b\\_5586478.html](http://huffingtonpost.com/bruce-kushnick/title-shopping-exposed-ve_b_5586478.html)

Joe Brodtkin, Ars Technica, "Title II hasn't hurt network investment, according to the ISPs themselves," 2017:

<https://arstechnica.com/information-technology/2017/05/title-ii-hasnt-hurt-network-investment-according-to-the-isps-themselves/>

<sup>12</sup> Bruce Kushnick, Huffington Post, "Net Neutrality Solved: Verizon's FiOS Rides over a Title II, Common Carriage, FTTP (Fiber-to-the-Premises) Telecommunications Network," 2014:

[http://huffingtonpost.com/bruce-kushnick/net-neutrality-solved-ver\\_b\\_5390789.html](http://huffingtonpost.com/bruce-kushnick/net-neutrality-solved-ver_b_5390789.html)

reclassification would stop broadband network investment and slow development.<sup>13</sup> Thus, the ISP appears to seek common carriage protection only where profitable. We strongly believe in seeing through this facade, and demand that cross-the-board common carriage rules be applied to ISPs.

In black letter law and regulatory history, Title II is a more accurate classification of BIAS. The distinction between telecommunication and information services stem from a series of FCC and court decisions during the rise of computer networking in the 1970s and 1980s.<sup>14</sup> A line was drawn between “basic” transmission services, described as “the offering of a pure transmission capability over a communications path that is virtually transparent in terms of its interaction with customer supplied information,” and the newer “enhanced services” that involve greater “computer processing” of the data transmitted.<sup>15</sup> The 1996 Act intended to regulate “basic” services under its Title II “telecommunications” regulations, while “enhanced” offerings went into the Title I “information services” bucket.

Simply put, no one signs up to Comcast or Spectrum for their transformational powers. Users contract BIAS providers to reach the world of content and applications available at the far ends of the internet, as fast as possible.<sup>16</sup> Thus, on its face, the average package that delivers home internet access has more in common with basic telecoms services than the enhanced offerings.

Not just good policy, the 2015 Title II classification fits best the definitions in the 1996 Telecommunications Act. The Title II Order recognizes that people direct their ISPs to transmit information to various points on the internet, including the servers of websites. To read into the Act a geographical component, where users must know and intend to send traffic to specific physical addresses, defies logic as well as the Commission’s own rulings. For example, the FCC maintains Title II classification of cellular telephony, whose users cannot be expected to direct their calls and texts to specific cell towers. Rather, the user knows the individual or entity understood to sit at the other end, and employs the provider to route traffic there. This is the role of ISPs: enabling us to connect and transmit our data without interference, as quickly and robustly as possible.

The distinction between more heavily regulated telecommunications services and freer information services accords with the technical and policy differences between the sectors.

---

<sup>13</sup> Amy Schatz, Recode, “Internet Providers Strike Back on Net Neutrality,” 2014:  
<https://recode.net/2014/5/13/11626818/internet-providers-strike-back-on-net-neutrality>

<sup>14</sup> Computer II”, Docket No. 20828, Final Decision, 77 FCC 2d 384, 1980:

<sup>15</sup> “Computer and Communications Industry Association v. Federal Communications Commission,” conclusion, para. 18, 1982:  
<http://openjurist.org/693/f2d/198/computer-and-communications-industry-association-v-federal-communications-commission>

<sup>16</sup> Jon Brodtkin, Ars Technica, “To kill net neutrality rules, FCC says broadband isn’t ‘telecommunications,’” 2017:  
<https://arstechnica.com/information-technology/2017/06/to-kill-net-neutrality-rules-fcc-says-broadband-isnt-telecommunications>

## i. Analysis: Difference between telecom services and internet applications

### **Telecom Services**

There are strong public interest reasons for regulating telecommunications services and imposing specific obligations such as neutrality. For instance:

- Telecommunications industries exploit scarce resources that belong to the “eminent domain” of states: namely telecommunications spectrum and in some cases infrastructure that was built by governments.<sup>17</sup> This earlier thinking of “scarcity” in broadcast spectrum is key to understanding the “must carry” regulations often enforced on telecommunications,<sup>18</sup> and cable TV and the “content quotas” that are imposed on audiovisual service providers.<sup>19</sup> There is a public interest in protecting freedom of expression in all its facets and pluralism via “positive discrimination” when private players are granted exclusive or semi-exclusive rights to use public resources such as radiofrequency spectrum and common telecom physical infrastructure.
- Additionally, the exploitation of public resources by telecommunications operators implies an economic advantage that is there from the beginning and that justifies regulations about investment quotas, universal service obligations, social tariffs, etc. This advantage is economy of scale.<sup>20</sup> This is particularly true these days when “triple-play” or “convergent” operators are appearing throughout the world. Not every company will be able to offer such efficient communications “bundles” or “packs”; meaning that the telecommunications markets have high barriers to entry and therefore are prone to cartelisation and concentration (lack of competition).

### **Internet Applications**

Meanwhile, in contrast:

- The internet is defined by abundance, not scarcity.<sup>21</sup> Even though there are services / protocols that serve the same function as telecommunications technologies (instant messaging, Voice over IP, video on demand, etc.), the reasons for regulating their use are different. The case for licensing-style regulatory intervention in the name of supporting either diversity or competition has not been made.

---

<sup>17</sup> This is especially true in the case of Latin America before the telecommunications liberalisation in the 90s.

<sup>18</sup> Alexandre Vuchot, Bird & Bird, “MustCarryRules,” 2003:

<https://twobirds.com/en/news/articles/2003/mustcarryrules>

<sup>19</sup> “Countries with massive domestic markets like the United States and India have considered there is no need to protect the output of their cultural sectors and have not introduced content regulation,” (Broadcasting Content Quotas- an International Overview)

[http://musicinaustralia.org.au/index.php?title=Broadcasting\\_Content\\_Quotas\\_%E2%80%94\\_An\\_International\\_Overview](http://musicinaustralia.org.au/index.php?title=Broadcasting_Content_Quotas_%E2%80%94_An_International_Overview)

<sup>20</sup> World Economic Forum, “What is the future of telecommunications in Latin America?” 2016:

<https://weforum.org/agenda/2016/06/has-telecom-privatization-in-latin-america-been-a-success/>

<sup>21</sup> Wired Staff, “New Rules For The New Economy,” 1997:

<https://wired.com/1997/09/newrules/>

- On diversity: On the internet, anyone who has access to the network can benefit from its neutral and open characteristics. Freedom and consumer choice are, by definition, often the main factor that decides what kind of content or service is popular.<sup>22</sup>
- Moreover, since there are no fixed quotas or quantitative limitations to content, actors who have difficulty getting their own media outlets, or whose dissident or minority viewpoints deter broadcasters, can reach interested communities on the internet.<sup>23</sup> In conclusion, the barrier of entry to the communications “market” on the internet is low enough that almost any interested party can operate a communications service or a media outlet, effectively supporting democratization of speech.
- On competition: In theory, economic actors “compete” to sell products or services that may offer similar value, and could serve as substitutes for one another. However, users are migrating in their choice of technologies rather than in the use of products or services; telecommunications services and services based on internet protocols are so different that they could barely be considered competing “substitutes.” Consider SMS vs. internet messaging apps like Viber, Signal, WhatsApp, or Snapchat; their business models are different (consumption vs. data exploitation), the technology they use is different, the barrier of entry to the market is different (and therefore the offering of alternatives is different), and their degree of availability to the public is different (there are messaging platforms that are open for everyone to use while others are closed or exclusive. Not having access to one of them does not imply endangering the right to communication; while not having access to SMS, for instance, leaves the user with very little or no available substitutes).

Title II authority remains a superior option for BIAS, and has successful track record in the wireless sphere. In 2007, the FCC employed Title II authority for voice and text roaming regulation.<sup>24</sup> Since implemented, the regulation has worked effectively and efficiently while wireless service has thrived.<sup>25</sup> Additionally, 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.<sup>26</sup> 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.

In word and deed, Title II continues to be the appropriate channel for increasingly essential broadband services.

---

<sup>22</sup> Censorship clearly limits access to information online, including through violations of neutrality, shutdowns and blocking of various forms, surveillance and its chilling effect, etc.

<sup>23</sup> This includes, but is not limited to indigenous populations, citizen journalists, LGBTI collectives, localised/multilingual content creators, and artists outside the copyright-driven production scheme.

<sup>24</sup> 47 C.F.R. § 20.12

<sup>25</sup> 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).

<sup>26</sup> *Verizon v. FCC*, 740 F.3d 623, 650 (D.C. Cir. 2014)

## 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.<sup>27</sup> 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.

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.

### A. Internet Conduct Standard

The Commission’s Title II Order created a standard intended to prohibit “current or future practices that cause the type of harms [the Commission’s] rules are intended to address,”<sup>28</sup> allowing it to prohibit practices that it determines unreasonably interfere with or unreasonably disadvantage the ability of consumers to reach the internet content, services, and applications of their choosing or of online content, applications and service providers to access consumers, per the NPRM.<sup>29</sup>

---

<sup>27</sup> Q&A on Network discrimination in Europe, Access, 2013:  
[https://accessnow.org/cms/assets/uploads/archive/docs/Access\\_QA\\_Footnotes\\_1.pdf](https://accessnow.org/cms/assets/uploads/archive/docs/Access_QA_Footnotes_1.pdf)

<sup>28</sup> Title II Order, 30 FCC Rcd at 5659, para. 135.

<sup>29</sup> Ibid

This Conduct Standard provides a basis for the clearer rules that business craves, and the stronger, forward-looking protection that users require. The Conduct Standard should be strengthened to more clearly eliminate the opportunity for price discrimination and business models that privilege ISPs to promote or demote certain types and sources of content.

## i. Zero rating and threats to the open internet

One of the newest threats to freedom of expression lies in so-called “zero rating” business models.

Zero rating programs manifest in different forms, the most frequent being “sub-internet” offers, where only a part of the internet is offered for “free,” and what we’re calling the “telco” model, where a telco prioritizes either its own content or that of third parties.<sup>30</sup> All forms of zero rating amount to price discrimination, and have in common their negative impact on users’ rights.

In the telco model, implemented by companies like Verizon, the provider gives preferential treatment to its own content, over whatever content might be independently created using its network. The telco model utilizes some form of QoS (Quality of Service) protocol to ensure that its content is given preferential treatment, and therefore always appears “smoother” and more reliable than competing content. This content can be video, music services, or other applications. Originally, QoS protocols were intended for internet users to dictate to the carriers what their preferences are for their own experience. These features were never intended to empower carriers to force their preferences on users through zero rating programs.

The second, and much more restrictive, model is the one used for sub-internet offers such as Facebook’s Free Basics program and others, which orchestrate a tightly controlled “walled garden” network. Here, tech companies insert themselves in the middle of all communications in partnership with a telecom carrier, and dictate everything that users can and cannot do on the network.

The sub-internet offers model puts technology companies who partner with telecom carriers to provide such programs in the middle of every network transaction. With current implementations of this model, users cannot do anything with any website or service without the company seeing their traffic and knowing what they are doing. By putting itself in the middle of every request and response over the network, the company can gain total access to the user’s behavior to build a detailed profile and have access to their communications history. Not only does this model dictate that all of the user’s traffic go through the company, but the company needs the user’s traffic to be unencrypted at that interception point. Otherwise it cannot use the user’s data to build a profile. This model therefore does not allow end-to-end (strong) encryption. Such encryption would let the user break out of the zero rating “jail.” With end-to-end encryption, the carrier or provider offering a zero rating program would not see what the user is doing, and this renders profile-building impossible.

---

<sup>30</sup> Estelle Massé, Gustaf Björkstén, Raman Jit Singh Chima, “Zero rating: a global threat to the open internet,” 2016: <https://accessnow.org/zero-rating-global-threat-open-internet>

Given the restrictions and control that zero rating programs impose, it seems likely there would be less innovation and less opportunity for internet users to participate in it. This is confirmed by the recent landmark empirical research report published by the Alliance for Affordable Internet (A4AI), which found that “zero rating did not bring most mobile internet users online for the first time.”<sup>31</sup> Moreover, the report found that the vast majority of users (82%) prefer access to the full internet with time or data limitations, if restrictions had to be imposed, than censored or filtered access. Limiting access to the full internet materially impacts low income users, who prefer even short-term or low-bandwidth access to an open, unrestricted internet, versus the restricted experience that zero rating provides.<sup>32</sup>

In sum, zero rating cedes control over the user experience to the telecom carrier — and potentially its business partners. Technologically, it relies on manipulation of the network, where providers guide or force the user to change the way they behave online, acting as gatekeepers to our digital identities. Several countries have banned zero rating programs. The Telecoms Regulatory Authority of India (TRAI) was one the first regulators to substantially look into the issue of zero rating. After extensive consultations, it passed what many have described as some of the strongest rules on zero rating — a comprehensive regulation restricting discriminatory differential pricing.<sup>33</sup>

Zero rating programs fail the Conduct Standard in several areas, per the factors identified in the 2015 Title II Order.<sup>34</sup> First, the programs take control out of the end user’s hands and place it firmly in the grip of the providers, who often wield it in consort with powerful content producers. The user cannot access the full internet or use it as “he or she sees fit.”<sup>35</sup> This collusion results in limited offerings interfering with the user’s freedom of expression and access to information.

Second, the FCC itself found in a 2016 report that zero rating practices require more effective regulatory oversight.<sup>36</sup> Commercial interests like innovation and competition suffer when ISPs get to pick and choose which edge providers or content types they want to promote or demote through price discrimination. “Given the powerful economic incentives of network operators to employ these practices to advantage themselves and their affiliates in various edge service markets,” FCC staff wrote, “we are equally concerned that – absent effective oversight – these practices will become more widespread in the future.”

---

<sup>31</sup> Alliance for Affordable Internet, “Digging into the Data: Is Zero-Rating Connecting the Unconnected?” 2016: <http://a4ai.org/is-zero-rating-really-bringing-people-online>

<sup>32</sup> Helani Galpaya, LIRNEasia, “Finally, some research on Zero Rated offers and users. And it’s surprising,” 2015: <http://lirneasia.net/2015/10/finally-some-research-on-zero-rated-offers-and-users-and-its-surprising/>

<sup>33</sup> Access Now, “Indian regulator stands up for Net Neutrality, rules against zero-rated services,” 2016: <https://accessnow.org/indian-regulator-stands-up-for-net-neutrality-rules-against-zero-rated-services/>

<sup>34</sup> See paras 138-145.

<sup>35</sup> 2015 Order at para 139

<sup>36</sup> FCC, Wireless Telecommunications Bureau Report: Policy Review of Mobile Broadband Operators’ Sponsored Data Offerings for Zero-Rated Content and Services, 2016: [https://transition.fcc.gov/Daily\\_Releases/Daily\\_Business/2017/db0111/DOC-342987A1.pdf](https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0111/DOC-342987A1.pdf)

Finally, consumers lack protection in zero rating schemes, which often require deep packet inspection and restrictive policing of data flows by ISPs. For these reasons, we submit that zero rating schemes represent unreasonable interference with the public's interest in the open internet and innovation online.

To prevent further harm, we recommend the FCC retain, strengthen, and enforce the Conduct Standard and other relevant regulations with the power to disallow zero rating programs.

## B. No Blocking Rule

The no blocking rule prohibits ISPs from excluding certain services and applications of competing market players. Specific examples of ISPs engaging in this kind of interference include:

- in 2008, the FCC condemned Comcast's practice of selectively targeting and interfering with connections of peer-to-peer applications;<sup>37</sup>
- Before late 2009, AT&T did not allow for VoIP applications to be used with 3G data on the iPhone.<sup>38</sup>
- Current internet policy in the United Kingdom mandates that all ISPs utilize default network blocking, which is meant to act as an opt-in service to protect children from viewing explicit materials. However, in practice the program is notoriously difficult to be removed from, and has mistakenly blocked the websites of women's health charities, florists, and HotWheels.com.<sup>39</sup>

This discriminatory and arbitrary practice threatened the benefits of an open and accessible internet.

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.<sup>40</sup> 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

---

<sup>37</sup> 23 FCC Rcd 13028, 13054 , 23 FCC Rcd 13028 (F.C.C. 2008)

<sup>38</sup> Ryan Singel, Wired, "AT&T Relents, Opens iPhone to Skype, VoIP," 2009:  
<http://wired.com/2009/10/iphone-att-skype>

<sup>39</sup> Ruth Coustick-Deal, "Blocked! How the Firewall of Britain is censoring the internet," 2014:  
<https://www.opendemocracy.net/ourkingdom/ruth-coustickdeal/blocked-how-firewall-of-britain-is-censoring-internet>

<sup>40</sup> Kenneth Corbin, Datamation, "See White House IP Chief Talks Tough on Online Piracy," 2010:  
<http://datamation.com/features/article.php/3905746/White-House-IP-Chief-Talks-Tough-on-Online-Piracy.htm>



percent of sites -19,000 of the 100,000 tested, a huge percentage - are blocked by one ISP or another.<sup>41</sup>

According to the NPRM, “The FCC has repeatedly found the need for a no-blocking rule in principle, asserting that ‘the freedom to send and receive lawful content and to use and provide applications and services without fear of blocking is essential to the Internet’s openness.’” We see no justification to deviate from this principle by rolling back clear, certain, and effective regulation against blocking.

## C. No Throttling Rule

The no throttling rule prevents ISPs from slowing 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, this prevents ISPs from compromising 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.<sup>42</sup>

Throttling practices by ISPs hinder competition online and contradict the innovation without permission principle. In 2014, Comcast forced Netflix into a deal after degrading the quality of the online service by throttling the connection speed. After months of complaints from Comcast users about a drop in quality of the Netflix streams being delivered to their homes, Netflix paid the company to restore speed and quality.<sup>43</sup> Comcast not only interfered in the network at the expense of users but also got paid twice to deliver access to an online service: once by the users, and once by Netflix. This gatekeeper behavior harms the competitiveness and economic benefits of U.S. online services, in turn damaging the public’s interest in an affordable, secure, and open internet.

## D. No Paid Prioritization Rule

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.”<sup>44</sup>

Paid prioritization can take different forms. Over the past years, zero rating — the practice of offering internet users free access to some, but not all, of the internet, resulting in unequal

---

<sup>41</sup> Pam Cowburn, ORG, “ORG’s Blocked project finds almost 1 in 5 sites are blocked by filters,” 2014: <https://openrightsgroup.org/blog/2014/blockedproject>

Blocked, 2014: <https://blocked.org.uk>

<sup>42</sup> Charlie Osborne, ZD Net, “Is your Internet provider throttling BitTorrent traffic? Find out,” 2014: <http://zdnet.com/article/is-your-internet-provider-throttling-bittorrent-traffic-find-out/>

<sup>43</sup> Shalini Ramachandran, WSJ, “Netflix to Pay Comcast for Smoother Streaming,” 2014: <https://wsj.com/articles/netflix-agrees-to-pay-comcast-to-improve-its-streaming-1393175346>

<sup>44</sup> Harold Feld, “Of CDNs, Netflix, Net Neutrality, and Cable Fu#\$@!ery.,” 2014: <http://wetmachine.com/tales-of-the-sausage-factory/of-cdns-netflix-net-neutrality-and-cable-fuery/>

access — has been growing.<sup>45</sup> In the U.S., Latin America and the European Union, telecoms companies have launched offers giving preferential treatment to specific content — often their own — over whatever content might be independently created using its network.<sup>46,47</sup> This type of network discrimination utilizes some form of QoS (Quality of Service) protocol to ensure that specific content is given preferential treatment, and therefore always appears “smoother” and more reliable than competing content.<sup>48</sup> Originally, QoS protocols were intended for internet users to dictate to the carriers what their preferences are for their own experience. Users could configure a router to pass information upstream to the carrier, designating which services mattered for them.<sup>49</sup> The expectation was that carriers would comply with a “best effort” to fulfill the user’s preferences. The reality was that while some enterprise “users” configured QoS on their internet-connected routers, few individuals made use of the QoS features that existed (and still exist) in domestic networking equipment. Carriers have argued that because QoS features exist in the internetworking protocols, it implies that protocol designers intended to implement zero rating. But this assumption is simply not true. These features were never intended to empower carriers to force their preferences on users through zero rating programs.

ISPs have also imposed data caps on internet access contracts while granting data allowance exceptions to their own proprietary streaming services.<sup>50</sup> In 2014, T-Mobile allowed customers to access specific streaming services without decreasing their individual data usage. Similarly, in 2016, AT&T announced that its video streaming system would not count against data caps, while Netflix would.<sup>51</sup> Any new or developing service will remain at a disadvantage<sup>52</sup>; generally only large, well-established companies or telcos’ own services can afford this preferential

---

<sup>45</sup> Estelle Massé, Gustaf Björkstén, Raman Jit Singh Chima, “Zero rating: a global threat to the open internet,” 2016: <https://accessnow.org/zero-rating-global-threat-open-internet>

<sup>46</sup> Jon Brodtkin, Ars Technica, “Sprint now zero-rating some video, joining AT&T, Verizon, and T-Mobile,” 2016:

<http://arstechnica.com/business/2016/05/sprint-now-zero-rating-some-video-joining-att-verizon-and-t-mobile/>

<sup>47</sup> <https://respectmynet.eu/>

<sup>48</sup> International Telecommunication Union (ITU), “World Conference on International Telecommunications (WCIT) Background Brief - Quality of Service and ‘Net Neutrality,’” 2012:

<http://itu.int/en/wcit-12/documents/wcit-background-brief11.pdf>

<sup>49</sup> Body of European Regulators of Electronic Communications (BEREC), “Guidelines for quality of service in the scope of net neutrality,” 2012:

[http://berec.europa.eu/eng/document\\_register/subject\\_matter/berec/regulatory\\_best\\_practices/guidelines/1101-berec-guidelines-for-quality-of-service-in-the-scope-of-net-neutrality](http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/1101-berec-guidelines-for-quality-of-service-in-the-scope-of-net-neutrality)

<sup>50</sup> Giusy Cannella, Raegan MacDonald & Jochai Ben-Avie, Access Now, “Net Neutrality-Ending Network Discrimination in Europe,” 2013:

[https://s3.amazonaws.com/access.3cdn.net/653b3b0adb37e88f4b\\_u7m6vw480.pdf](https://s3.amazonaws.com/access.3cdn.net/653b3b0adb37e88f4b_u7m6vw480.pdf)

Citing to: David Meyer, Gigaom, “Deutsche Telekom’s “anti-net- neutrality” plans alarm German government,” 2013:

<https://gigaom.com/2013/04/25/deutsche-telekoms-anti-net-neutrality-plans-alarm-german-government/>

<sup>51</sup> Jon Brodtkin, Ars Technica, “Verizon’s mobile video won’t count against data caps—but Netflix does,” 2016:

<http://arstechnica.com/business/2016/02/verizons-mobile-video-wont-count-against-data-caps-but-netflix-will/>

<sup>52</sup> Jared Newman, Time, “T-Mobile’s Unlimited Music Streaming Is the Worst for Net Neutrality,” 2014:

<http://time.com/2901142/t-mobile-unlimited-music-net-neutrality/>

treatment. Thus, where ISPs essentially lord over a certain market, like music streaming services, its network discrimination discourages innovation and causes a lack of competition.

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. 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.<sup>53</sup> 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.<sup>54</sup> 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.

Access Now believes that not only should be paid prioritization rule be kept, but it should be intensified to protect against deep packet inspection.

Under the no paid priority rule, 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 is 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.<sup>55</sup> Under “paid priority” schemes, DPI could help ISPs monitor traffic to decide which content users want, and when they want to download it, leading to discriminatory pricing, throttling, and gouging.

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., 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.

---

<sup>53</sup> Kirsten Fiedler and Joe McNamee, EDRI, “Net Neutrality,” 2013: [http://edri.org/files/paper08\\_netneutrality.pdf](http://edri.org/files/paper08_netneutrality.pdf) Citing to: Body of European Regulators of Electronic Communications (BEREC), “A view of traffic management and other practices resulting in restrictions to the open Internet in Europe,” 2012: [https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC\\_2.pdf](https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf) at page 12

<sup>54</sup> James Bamford, Wired, “The NSA Is Building the Country’s Biggest Spy Center (Watch What You Say),” 2012: [http://wired.com/2012/03/ff\\_nsadatacenter/all/](http://wired.com/2012/03/ff_nsadatacenter/all/)

<sup>55</sup> Andreas Kuehn & Milton Mueller, Syracuse University - School of Information Studies, “Profiling the Profilers: Deep Packet Inspection and Behavioral Advertising in Europe and the United States,” 2012: [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2014181](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2014181)

See also: Telegraph, “BT and Phorm: how an online privacy scandal unfolded,” 2011: <http://telegraph.co.uk/technology/news/8438461/BT-and-Phorm-how-an-online-privacy-scandal-unfolded.html>.

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.<sup>56</sup> 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 time) or insofar as network management purposes or legal orders prescribe.<sup>57</sup> Furthermore, the Dutch telecommunications watchdog inspects providers to ensure compliance. This landmark Dutch law could be studied as a starting point for regulations not only prohibiting network discrimination in the U.S. but also empowering users to protect and control their data.

## E. Transparency Rule

Access Now 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 counted 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.<sup>58</sup> Transparency is the first step, but definitely not the last step, to achieving net neutrality.

---

<sup>56</sup> Giusy Cannella, Raegan MacDonald & Jochai Ben-Avie, Access Now, "Net Neutrality-Ending Network Discrimination in Europe," 2013:

[https://s3.amazonaws.com/access.3cdn.net/653b3b0adb37e88f4b\\_u7m6vw480.pdf](https://s3.amazonaws.com/access.3cdn.net/653b3b0adb37e88f4b_u7m6vw480.pdf)

Citing to: Bits of Freedom, "Translations of key Dutch internet freedom provisions," (Dutch Telecommunications Act) 2011:

<https://www.bof.nl/2011/06/27/translations-of-key-dutch-internet-freedom-provisions/>

<sup>57</sup> Access Now, "To Regulate or Not to Regulate, Is That The Question?: A Roadmap to Smart Regulation of the Internet," 2011: [https://s3.amazonaws.com/access.3cdn.net/62a6294b6db705f68c\\_gcm6iynrv.pdf](https://s3.amazonaws.com/access.3cdn.net/62a6294b6db705f68c_gcm6iynrv.pdf)

Citing to: Dutch Parliament, "Artikel 11.2a Telecommunicatiewet," 2016:

<http://maxius.nl/telecommunicatiewet/artikel11.2a>

<sup>58</sup> FCC IATD, "Internet Access Services: Status as of December 31, 2012," 2013:

[https://apps.fcc.gov/edocs\\_public/attachmatch/DOC-324884A1.doc](https://apps.fcc.gov/edocs_public/attachmatch/DOC-324884A1.doc) at page 9 - table 5(a)

See also: Gizem Orbey, Harvard Journal of Law and Technology, "Susan Crawford Explains the Significance of the Comcast-Time Warner Cable Merger," 2014:

<http://jolt.law.harvard.edu/digest/susan-crawford-explains-the-significance-of-the-comcast-time-warner-cable-merger>

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.<sup>59</sup> 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.

Providing this type of information, through corporate “transparency reports,” is becoming a best practice for internet platforms and telecom providers.<sup>60</sup> 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.

---

<sup>59</sup> Kim Zetter, Wired, “See Feds ‘Pinged’ Sprint GPS Data 8 Million Times Over a Year,” 2009:

<http://wired.com/2009/12/gps-data>;

David Kravets, Wired, “Which Telecoms Store Your Data the Longest? Secret Memo Tells All,” 2011:

<http://wired.com/2011/09/cellular-customer-data/>;

Glenn Greenwald, The Guardian, “NSA collecting phone records of millions of Verizon customers daily,” 2013:

<http://theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>;

Barton Gellman and Laura Poitras, Washington Post, “U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program,” 2013:

[http://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](http://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)

<sup>60</sup> See e.g.: Apple transparency reports, 2013-2016: <https://www.apple.com/privacy/transparency-reports/>;  
AT&T transparency report, 2016:

<http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html>;

Google transparency report, 2009-2016: <https://google.com/transparencyreport/userdatarequests/US/>;

Verizon transparency report, US-International: <http://www.verizon.com/about/portal/transparency-report/>

## F. Additional considerations regarding the Open Internet Rules

With regard to so-called “over the top services” or OTTs, applying legacy telecommunications regulation to internet content could harm the open internet and the principles that sustain the enjoyment of digital rights, in particular the principles of permissionless innovation and end-to-end accessibility. Economically, application of these regulations to OTTs would raise barriers to enter the digital market; greater competition is most needed in the broadband access, not content, market.

From an economic view, telecom services and OTT applications are not perfect substitutes for one another. They are based in different technologies that relate to state-level interests in a different manner with respect to telecommunications regulation. Therefore, the regulatory approach to them should be different and find basic premises that put users’ rights first.

Particularly, we should counter the trend towards the commoditization of the internet, where applications would be licensed separately and offered in “bundles” with internet connection packs – the trend we are seeing with zero rating programs. Keeping the internet free, open, neutral, and interoperable is what enabled the growth and development of this technology.

Any regulation that deals with OTT services in particular should be fact-based and defend and extend the rights of users, without jeopardizing the core principles that keep the internet free and open for innovation.

Examples of regulation that would benefit users and protect rights include:

- Safeguarding strong neutrality rules to avoid arbitrary interference discrimination, including price differentiation on the basis of applications and protocols;
- Protecting principles to keep the internet open to innovation and free expression, such as the end-to-end principle and open and interoperable protocols;
- Advancing meaningful data protection and privacy oversight and measures to safeguard the interests of users;
- Extending connectivity through rights-respecting, equitable programs and infrastructure;
- Fighting corporate and government surveillance mechanisms and fostering the improvement of technical measures to protect privacy;
- Maintaining clear emergency services communication channels and protocols; and
- Holding companies accountable to their human rights obligations.

The Commission requests comments on how it should view any additional guidance explaining the definition of non-broadband Internet access service data services that fall outside the scope of the rules.

The lack of a clear definition of non-broadband internet access service data services 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.

### **3. Harms resulting from classification of BIAS as an Information Service**

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. Title II classification puts the FCC's full weight behind guarantees of a level playing field for lawful web content, platforms, and emerging technologies. The benefits flow widely: from churches live-streaming services to rural users,<sup>61</sup> and racial justice advocates organizing across the country,<sup>62</sup> content producers of all stripes and sizes make the internet a place where established platforms and startups of all stripes want to compete, and users want to connect. With such diversity and democracy in action, ISPs cannot be expected and should not be empowered to mediate between content types, sources, destinations, or sizes while still maintaining the public's interest. Strong regulation, with appropriate forbearance, enable the FCC to protect net neutrality in the U.S. and set a clear precedent for global protection of human rights online.

Evidence points to the need for a stronger regulatory framework for BIAS than Title I provides.

#### **A. 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

---

<sup>61</sup> Brian Pellot, Religion News Service, "Interfaith leaders find common ground promoting Internet freedom," 2015: <http://religionnews.com/2015/08/12/net-neutrality-interfaith-leaders-internet-freedom>

<sup>62</sup> Matt Sledge, Huffington Post, "Police Reform Organizers Pitch Net Neutrality To FCC," 2015: [http://huffingtonpost.com/2015/01/09/net-neutrality-fcc\\_n\\_6446302.html](http://huffingtonpost.com/2015/01/09/net-neutrality-fcc_n_6446302.html)

current non-priority infrastructure to make prioritized options seem more attractive.<sup>63</sup> 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.<sup>64</sup> 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.<sup>65</sup> Further, the FCC investigated why users received varied and throttled access to the popular video service Netflix<sup>66</sup> via ISPs that offered competing services - a scenario that merits particular scrutiny for evidence of network discrimination. Of 51 peering partners, 12 had congested networks. Of those 12, 6 are unwilling to make upgrades. All six are large broadband consumer networks with a dominant or exclusive market share, and five are U.S. providers.

## B. 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 are low but the potential for technology improvement is huge.<sup>67</sup> 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 the earlier version of the FCC net neutrality rules proposed in 2014, that his firm will “stay away from” startups working on video and media business models.<sup>68</sup> Net neutrality

---

<sup>63</sup> See page 4, 16, 17, 22, and 32: Choi, Jay Pil and Kim, Byung-Cheol, RAND Journal of Economics, Vol. 41, No. 3, “Net Neutrality and Investment Incentives,” 2010: Available at SSRN: <http://ssrn.com/abstract=1285639>

<sup>64</sup> See: Sam Gustin, Time, “Netflix Pays Verizon in Streaming Deal, Following Comcast Pact,” 2014: <http://time.com/80192/netflix-verizon-paid-peering-agreement/>; Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014); Jon Brodtkin, Ars Technica, “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/>

<sup>65</sup> Mark Taylor, Level 3 Communications, Observations of an Internet Middleman, 2014: <http://blog.level3.com/global-connectivity/observations-internet-middleman/>

<sup>66</sup> Richard Lawler, Engadget, “The FCC is looking into Netflix’s issues with Comcast and Verizon,” 2014: <http://engadget.com/2014/06/13/fcc-is-looking-into-netflixs-issues-with-comcast-and-verizon/>

<sup>67</sup> Choi, Jay Pil and Kim, Byung-Cheol, RAND Journal of Economics, Vol. 41, No. 3, “Net Neutrality and Investment Incentives,” 2010: Available at SSRN: <http://ssrn.com/abstract=1285639>

<sup>68</sup> Zach Epstein, BGR, “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/>



regulation would restore investment incentives for edge providers by alleviating their fear of potentially harmful ISP network discrimination.

One area of new technology where threats of network discrimination proliferate is 5G. Named for the 5th generation of mobile networks, 5G would bring much-needed increases in internet speed and coverage for people across the global wireless system. The Next Generation Mobile Networks Alliance has defined a 5G network standard to have data rates of 100 megabits per second for metropolitan areas, among other indicators promising more efficient spectrum, wider coverage areas, and increased capacity for wireless sensors. The standard is seen to welcome the Internet of Things and an ever-increasing number of internet-connected products and services, such as connected cars and e-health.

In the summer of 2016, a group of 20 telecoms operators and hardware manufacturers published a “5G Manifesto”<sup>69</sup> in which they threatened to withhold 5G investment unless the European Union waters down its rules protecting network neutrality. In response, a coalition of more than 30 NGOs from around the world sent an open letter<sup>70</sup> to policy-makers encouraging them to support the development and implementation of robust net neutrality rules alongside the deployment of high-quality broadband and next-generation networks. Despite this outcry, the EU Commission has been looking into the development of a Gigabit Society through high-capacity networks for the “delivery of video and audio content in gaming and streaming,” which could lead to the creation of separate fast lanes on the network that would contradict its neutrality provisions established in EU law in November 2015.<sup>71</sup>

Threats such as those made in the EU “5G Manifesto,” are unsubstantiated and represent further abuses of power from the telecommunications industry, which unfortunately are not confined to the European continent. Given their control of access to the network, operators already have a significant advantage over online services; something that network neutrality rules are attempting to mitigate to avoid abuses and discriminatory practices.

In fact, the principles on which net neutrality is based, including innovation without a need to obtain permission, end-to-end connectivity, transparency, and nondiscrimination, are essential for emerging products and services like 5G and IoT. Net neutrality rules will ensure that the number of innovative internet-based services and applications will continue to increase. With global demand for faster and better access to the internet on the rise, internet access providers will continue to have a strong incentive to develop and invest in enhanced network capacity for all people – and things. This so-called “virtuous circle” illustrates the long-term economic benefit for telecommunications companies to invest in an open and free infrastructure.

---

<sup>69</sup> BBC, “Telecoms companies unite to sign 5G manifesto,” 2016:  
<http://bbc.com/news/technology-36763903>

<sup>70</sup> Estelle Massé and Fanny Hidvegi, Access Now, “EU Commission’s plan for a Gigabit society raises concerns for Net Neutrality,” 2016:  
<https://www.accessnow.org/eu-commissions-plan-gigabit-society-raise-concerns-net-neutrality/>

<sup>71</sup> European Commission, “Improving connectivity and access,”  
<https://ec.europa.eu/digital-single-market/en/policies/improving-connectivity-and-access>

## C. Uncertain grounds for 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.<sup>72</sup> 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.<sup>73</sup>

The NPRM claims that the regulatory burden of the 2015 Title II Order, and the threat of regulatory enforcement, has resulted in negative consequences for American consumers, including depressed broadband investment and reduced innovation. A flurry of new studies and articles touch on broadband infrastructure investment since the 2015 introduction of the Title II Order. For example, Free Press finds increased capital expenditure by ISPs in 2015-2016, compared with the 2013-2014 period.<sup>74</sup> Other studies show a mix of greater and less infrastructure spending,<sup>75</sup> but nothing outside the realm of industry trends, including the slowdown following LTE buildout, or that can be pinpointed to the Title II Order.<sup>76</sup> Anecdotally, Verizon's CEO denies that current regulations direct its investment strategy.<sup>77</sup> The CEO of ISP Sonic notes that it has continued its "growth efforts, including fiber construction," and continues to adhere to net neutrality practices.<sup>78</sup>

For their part, investors and small businesses have clearly expressed their interest in strong network neutrality rules. Open internet policies "help drive the economy, encourage innovation

---

<sup>72</sup> See: Access Now, "The Importance of (Real) Net Neutrality for Investment," 2013:

[https://s3.amazonaws.com/access.3cdn.net/fb7263bc7a41434b1c\\_ktm6bnw0b.pdf](https://s3.amazonaws.com/access.3cdn.net/fb7263bc7a41434b1c_ktm6bnw0b.pdf);

Brian Williamson, David Black, and Thomas Punton, Plum, "The Open Internet - A platform for Growth, 2011:

[http://downloads.bbc.co.uk/aboutthebbc/insidethebbc/howwework/reports/pdf/plumbriefing\\_oct2011.pdf](http://downloads.bbc.co.uk/aboutthebbc/insidethebbc/howwework/reports/pdf/plumbriefing_oct2011.pdf)

<sup>73</sup> Access Now, "The Importance of (Real) Net Neutrality for Investment," 2013:

[https://s3.amazonaws.com/access.3cdn.net/fb7263bc7a41434b1c\\_ktm6bnw0b.pdf](https://s3.amazonaws.com/access.3cdn.net/fb7263bc7a41434b1c_ktm6bnw0b.pdf)

<sup>74</sup> Company SEC Filings (10-Ks, Financial Supplements) 2013-2016:

[https://www.freepress.net/sites/default/files/resources/internet\\_service\\_providers\\_capital\\_expenditures\\_2013-2016\\_reported\\_as\\_of\\_2\\_27\\_17.pdf](https://www.freepress.net/sites/default/files/resources/internet_service_providers_capital_expenditures_2013-2016_reported_as_of_2_27_17.pdf)

<sup>75</sup> Hal Singer, "2016 Broadband Capex Survey: Tracking Investment in the Title II Era" 2016:

<https://haljsinger.wordpress.com/2017/03/01/2016-broadband-capex-survey-tracking-investment-in-the-title-ii-era/>

<sup>76</sup> Klint Finley, Wired, "The New FCC Chairman's plan to undermine net neutrality," 2017:

<https://www.wired.com/2017/03/new-fcc-chairmans-plan-undermining-net-neutrality/>

<sup>77</sup> Matt Ellis-Verizon CFO, Verizon 4Q 2016 Quarter Earnings Conference Call Webcast, 2017 ("We're making investments that are for 10-plus years and I think our record stands for itself, that irrespective whoever the administration is run by and the regulatory regime, that we are effective. And that will continue to be how we focus our investments"):

<https://www.verizon.com/about/investors/quarterly-reports/4q-2016-quarter-earnings-conference-call-webcast>.

<sup>78</sup> Dane Jasper, Sonic (ISP), "Sonic Statement on Net Neutrality," 2014:

<https://corp.sonic.net/ceo/2014/11/12/sonic-statement-on-net-neutrality/>

and reward investors,” one group of investors and venture capitalists commented to the FCC.<sup>79</sup> Likewise, more than 1,000 small and medium-sized businesses from all 50 states recently sent a letter to Chairman Ajit Pai in support of the existing Title II classification of BIAS. “We also depend on an open Internet—including enforceable net neutrality rules that ensure big cable companies can’t discriminate against people like us,” the businesses wrote. “We’re deeply concerned with your intention to undo the existing legal framework.”<sup>80</sup>

In 2017, a group of 20 investors representing \$190 billion in assets told the FCC they oppose changes to the net neutrality rules. An internet that “guarantees fair and equal treatment is a core driver of America’s economic growth,” they said. “We believe network neutrality principles are critical to that process.... As investors, we find no evidence that the Commission’s 2015 Open Internet order has caused publicly-held ISPs to reduce their investment in broadband networks.”<sup>81</sup> They cited evidence from multiple public statements by corporate executives of the leading ISPs as well as data the companies supplied in their filings to the Securities and Exchange Commission.

Like Chairman Pai, ISPs have claimed that net neutrality regulation discourages investment, saying “free riders” congest networks without paying extra.<sup>82</sup> Here, ISPs are willfully ignoring what users really pay for – they “don’t buy fat pipes, they buy applications and content that require fat pipes.”<sup>83</sup> 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.<sup>84</sup> Thus, regulation appears to boost the incentive for the ISP to increase overall capacity by 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.

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

---

<sup>79</sup> Open MIC, “Investors Urge FCC to Adopt Net Neutrality Rules, Reclassify Broadband Internet under Title II,” 2014:

<http://www.openmic.org/issue-articles/2016/7/11/investors-urge-fcc-to-adopt-net-neutrality-rules-reclassify-broadband-internet-under-title-ii>

<sup>80</sup> Startups for Net Neutrality, “Letter to Federal Communications Commission (FCC) Chairman Ajit Pai,” 2017: <http://engine.is/startups-for-net-neutrality>.

<sup>81</sup> OpenMic, Investors Representing \$190 Billion in Assets Oppose FCC’s Proposed Changes to Net Neutrality Rules, 17 July 2017:

[www.openmic.org/issue-articles/2017/7/14/investors-representing-190-billion-in-assets-oppose-fccs-proposed-changes-to-net-neutrality-rules](http://www.openmic.org/issue-articles/2017/7/14/investors-representing-190-billion-in-assets-oppose-fccs-proposed-changes-to-net-neutrality-rules)

<sup>82</sup> Arshad Mohammed, “Verizon Executive Calls for End to Google’s ‘Free Lunch,’” 2007:

<http://washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020601624.html>

<sup>83</sup> Commissioner Robert. M. McDowell, “Address to the Broadband Policy Summit III, Arlington, VA, at 13-14” 2007: [https://apps.fcc.gov/edocs\\_public/attachmatch/DOC-273742A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/DOC-273742A1.pdf)

<sup>84</sup> Choi, Jay Pil and Kim, Byung-Cheol, RAND Journal of Economics, Vol. 41, No. 3, “Net Neutrality and Investment Incentives,” 2010: Available at SSRN: <http://ssrn.com/abstract=1285639>

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.<sup>85</sup> Most of us have about as many options for home garbage pick-up as broadband providers.

## D. More opaque peering and interconnection

The FCC seeks “to relinquish any authority over Internet traffic exchange.” 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 often regards broadband providers who effectively operate terminal monopolies. But to be effective, the FCC 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 Title II Order, the Commission took care not to harm 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 focused 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 retain stringent transparency rules to these provisioning arrangements, by requiring that any contract governing interconnection or exchange of traffic between networks or providers be disclosed to the FCC on a general basis, if not made public. Before the Title II Order, the Commission already began requesting the details of such agreements on an individual basis, seeing the threat of dominant players bullying edge providers borne out.<sup>86</sup>

Consumers have a right to know how upstream agreements are affecting the services they pay for and the information they can access. By retaining Title II classification, and enforcing disclosure and scrutiny of interconnection agreements, the Commission ensures that users and edge providers have adequate knowledge and representation in the interconnection marketplace.

## E. Obstacles to mobile broadband access and equity

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

---

<sup>85</sup> FCC IATD, “Internet Access Services: Status as of December 31, 2012,” 2013: [https://apps.fcc.gov/edocs\\_public/attachmatch/DOC-324884A1.doc](https://apps.fcc.gov/edocs_public/attachmatch/DOC-324884A1.doc)

<sup>86</sup> Jon Brodtkin, Ars Technica, “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/>

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.

Access Now insists that, given the maturation of mobile broadband since 2010, the Commission should retain the most comprehensive anti-blocking rule possible. In particular, mobile BIAS providers shall not block consumers from accessing websites, subject to reasonable network management; nor shall such provider block applications, subject to reasonable network management. This discrimination distorts competition and interferes with users' ability to use the application or services of their choice. To increase incentives to innovate, support end to end connectivity, and empower users to decide what services they want to access, practices such as blocking should be clearly prohibited across mobile and fixed networks.

Why? For one, wireless broadband is getting more popular, and essential, in the U.S. In 2013, the Pew Research Center reported noted that 91% of Americans owned cell phones,<sup>87</sup> a number that has risen to 95%.<sup>88</sup> More vulnerable and marginalized users, including younger adults, non-whites and lower-income Americans, are more likely than others to rely on mobile to get online.<sup>89</sup> This latter category, a growing group, encompasses users at risk.

Second, the world is going mobile. Penetration rates of mobile broadband subscriptions top 41% in developing nations; many citizens in developing countries are getting their first experience of the internet through mobile devices.<sup>90</sup> Affordability is an important component, and mobile is more often cheaper than fixed broadband.<sup>91</sup> However, these new users often encounter a restricted internet without end-to-end connectivity to sites and services. India's adoption rate is rising quickly,<sup>92</sup> for example, yet so has the incidence of partial and full internet shutdowns, with 69 shutdowns and rising from 2010,<sup>93</sup> with a total of 31 in 2016 itself.<sup>94</sup>

A weaker 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.

---

<sup>87</sup> Maeve Duggan and Aaron Smith, Pew Research Center, "Cell Internet Use 2013," 2013:

[http://pewinternet.org/files/old-media//Files/Reports/2013/PIP\\_CellInternetUse2013.pdf](http://pewinternet.org/files/old-media//Files/Reports/2013/PIP_CellInternetUse2013.pdf)

<sup>88</sup> Pew Research Center, "Internet/Broadband Fact Sheet," 2017:

<http://pewinternet.org/fact-sheet/internet-broadband>

<sup>89</sup> Pew Research Center, "Internet/Broadband Fact Sheet," 2017:

<http://pewinternet.org/fact-sheet/internet-broadband>

<sup>90</sup> Brahim Sanou, ITU, "ICT Facts and Figures 2016," 2016:

<http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf>

<sup>91</sup> Brahim Sanou, ITU, "ICT Facts and Figures 2016," 2016:

<http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf>

<sup>92</sup> Nandita Mathur, Live Mint, "India's Internet industry to double by 2020: report," 2017:

<http://www.livemint.com/Industry/8JkjSAVDJvU8YsNW11JiiJ/Indias-Internet-industry-to-double-by-2020-report.html>

<sup>93</sup> Centre for Communication Governance - National Law University Delhi, Infographic on Internet Shutdowns in India,

<https://keepusonline.in/content/images/2017/03/-CCG-NLU--Internet-Shutdown-Infographic.png>

<sup>94</sup> Software Freedom Law Centre - India, Internet Shutdowns, <https://internetshutdowns.in/>

approach to regulation of digital issues often serves as a point of reference. 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, into the future.

## 4. Effects on regulatory structures created by the Title II Order

Per the NPRM, the Federal Trade Commission (FTC) traditionally protected the privacy of broadband consumers. The FCC proposes to return jurisdiction over internet service providers' privacy practices to the FTC and seeks comments on this proposal.<sup>95</sup>

Stronger regulation protecting user privacy is urgently needed. The FCC's proposal to reverse course and return jurisdiction on privacy in telecommunications to the FTC represents a complete failure of leadership and foresight in this crucial area of the economy. Abdicating authority to the ill-equipped FTC will harm consumers and enable more damaging data security breaches, reducing trust in the entire internet economy. We fully oppose this proposal.

In 2016, the FCC voted to approve historic rules that would require broadband internet service providers to extend privacy and security protections to users. The FCC had received more than 275,000 comments on its proposal, including from Access Now.<sup>96</sup> The final rules<sup>97</sup> offered users the protections and respect for privacy that the industry has too often failed to provide on its own.

One of the major benefits of the rules were protections for web browsing data. In 2015, we reported that mobile broadband providers were using "supercookies" to track people's web browsing habits.<sup>98</sup> The tracking has been happening surreptitiously, without providers asking subscribers to opt-in and, in some cases, without even offering a way to opt-out. Yet web browsing habits can reveal deeply personal details about our lives. The FCC eventually did

---

<sup>95</sup> NPRM, pages 22-23

<sup>96</sup> Access Now, "Open letter to Ms. Marlene H. Dortch-Secretary FCC," 2016: <https://accessnow.org/cms/assets/uploads/2016/05/NPRM-PrivacyofBroadbandCustomers--Access-Now.pdf>

<sup>97</sup> FCC, "FCC 16-148," 2016: [https://transition.fcc.gov/Daily\\_Releases/Daily\\_Business/2016/db1103/FCC-16-148A1.pdf](https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1103/FCC-16-148A1.pdf)

<sup>98</sup> Nader Ammari, Gustaf Björkstén, Peter Micek, and Deji Olukotun, Access Now, "The Rise of Mobile Tracking Headers: How Telcos Around the World Are Threatening Your Privacy," 2015: <https://accessnow.org/cms/assets/uploads/archive/AIBT-Report.pdf>

penalize Verizon for this violation of user privacy and reasonable expectations.<sup>99</sup> The subsequent rules did therefore require broadband providers to get the user's affirmative consent before using their "sensitive" data.

The new rules further protected user privacy and security by requiring that providers:

- transparently disclose information about their privacy practices;
- get opt-in consent before using or sharing "sensitive" data — including the content of communications, web browsing data, and app usage history;
- give users the chance to opt-out from sharing and use of other, "non-sensitive" data, such as tier-level of service;
- take "reasonable measures" to protect security; and
- notify users if there is a data breach that can cause harm.

## A. Risks to the fundamental right to privacy

The fundamental right to privacy is recognized in international treaties endorsed by the United States, including the International Covenant on Civil and Political Rights.<sup>100</sup> The United Nations (UN) has applied human rights obligations to businesses in the Guiding Principles on Business and Human Rights (Guiding Principles), which asserts that governments have a duty to ensure that businesses in their territory respect human rights, including through regulation.<sup>101</sup> The Guiding Principles were unanimously endorsed by the UN Human Rights Council on June 16, 2011 in a resolution cosponsored by the U.S. government.<sup>102</sup> For their part, the OECD Guidelines for Multinational Enterprises specifically advise corporations to "take reasonable measures to ensure the security of personal data that they collect, store, process, or disseminate."<sup>103</sup>

Trust and certainty in the internet economy depends on widespread respect and regulatory safeguards for this human right. The FCC has increasingly worked to protect and enforce rights to privacy and freedom of expression online in recent years, and we look for continued international leadership in this process.

The FTC's post-hoc approach is ill-suited to set norms or foresee emerging threats to communications privacy. Broadband service providers have uniquely powerful, privileged access to our personal information. They are the ones that transfer our internet traffic, and they have direct access to every intimate thing we do and say online. This access will only grow as

---

<sup>99</sup> Verizon v. FCC, 740 F.3d 623, 650 (D.C. Cir. 2014)

<sup>100</sup> International Covenant on Civil and Political Rights art. 17 Dec. 16, 1966, S.Treaty Doc. No. 95-20, 6 I.L.M. 368, 999 U.N.T.S. 171

<sup>101</sup> Ibid. at 4.

<sup>102</sup> United States Department of State, Bureau of Democracy, Human Rights, and Labor, "U.S. Government Approach on Business and Human Rights," 2013:

<http://humanrights.gov/wp-content/uploads/2013/06/usg-approach-on-business-and-human-rights-update-djune2013.pdf>

<sup>103</sup> The Organisation for Economic Co-operation and Development, "VIII. Consumer Interests," 2011: <http://mneguidelines.oecd.org/2011ConsumerInterests.pdf>

we begin to use devices that are internet-enabled, and the data generated in an “Internet of Things” world will be even more intimate.

With its broadband privacy rules, the FCC had sent an important message, not just to broadband providers but to all companies, about the fundamental importance of protecting our privacy and security. Moreover, U.S. recognition of data privacy helped reinforce recognition worldwide of the value of frameworks that protect internet users.

To send enforcement to the FTC would do a disservice to internet users in the U.S. and set a weak example for other nations looking to update their protections for the human right to privacy online.

## 5. Conclusion

The open internet has enabled greater access to information and more robust opportunity to exercise human rights than any previous technology or system. As more people in the U.S. and around the world depend on internet-connected technology to earn a livelihood, secure an education, connect with family and friends, and advocate for their rights, and greater economic pressures come to bear on its privately owned and operated structures, regulators like the FCC have an awesome responsibility to protect the public interest and define the bounds of acceptable behavior. We support the FCC’s mission to promote competition, innovation, and investment in broadband services and facilities, and ensure that new technologies flourish alongside diversity and localism. We have shown and firmly believe that Title II classification of BIAS is the best and most appropriate way for the FCC to succeed in achieving its mission in the digital age.

Access Now ([www.accessnow.org](http://www.accessnow.org)) is an international organization that defends and extends the digital rights of users at risk. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

For more information, contact:

**Peter Micek**  
General Counsel | Access Now  
[peter@accessnow.org](mailto:peter@accessnow.org)