Mexico City, March 6, 2020

To the Commissioners of the Federal Telecommunications Institute,

Access Now is an international non-profit organization that defends and extends the digital rights of users at risk around the world. Part of our work consists of providing analysis and comments on issues like Net Neutrality, connectivity, privacy, and other related topics around the world. We appreciate the opportunity to submit these comments, with support from Electronic Frontier Foundation, Fight for the Future, National Hispanic Media Coalition, New America's Open Technology Institute, and Public Knowledge on the Federal Telecommunications Institute's (IFT) "Draft Guidelines for traffic management and internet administration that must be subject to the concessionaire and authorized who provide internet access services" (Draft Guidelines).

1. Introduction

Strong Net Neutrality protections are key in promoting human rights online. The internet is an important gateway through which fundamental rights can be realized, notably the freedoms of expression and association, and the rights to access culture and education. The greater availability and effective use of the services provided through internet access encourages social inclusion, expression, communication, education, innovation, wealth creation, productivity, finding employment, and good governance.[1] Universal internet access is a global objective shared by essentially all members of society. The Global Sustainable Development Goals reflect this in objective 9.C, which sets a goal to "significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries."[2] Mexico itself has been investing in reforming its telecommunications market since 2013.[3]

For the benefits of information and communications technologies to spread equitably and freely, people must be able to access online content without undue interference from their internet service provider (ISP). This is where strong Net Neutrality protections, enforced by a governmental body, are critical.

The IFT's Draft Guidelines are a start, however, they are insufficient to protect Mexican users. Specifically, the Draft Guidelines (1) will allow the government to shut down the internet and

[1] Organization for Economic Cooperation and Development (OECD) and Inter-American Development Bank (IDB) (2017), Broadband policies for Latin America and the Caribbean: A manual for the digital economy, http://www.oecd.org/internet/broadband/lac-digital-toolkit/Home/LAC-Broadband-Toolkit-ESP-Excerpt.pdf.
[2] United Nations, Sustainable Development Goals, Goal 9.C, https://www.un.org/sustainabledevelopment/es/infrastructure.
[3] Verena Weber, Mexico Telecom Reform: Into the "Last Mile," OECD Observer, http://oecdobserver.org/news/fullstory.php/aid/5910/Mexico_telecom_reform:_into_the__93last_mile_94.html.

should not, (2) will insufficiently protect Net Neutrality by allowing ISPs to engage in differential traffic management, (3) fail to address privacy, and (4) do not require sufficient transparency.

2. The IFT should not allow or facilitate internet shutdowns or permit intentional disruption of internet services.

The Draft Guidelines should not enable internet shutdowns or allow internet services to be disrupted. Articles 5(III) and 5(IV) state that an ISP may implement traffic management policies that would enable internet shutdowns if there is an "[e]mergency or national security situation" or "[a]t the express request of the competent authority."[4] Rules that allow governments to intentionally disrupt the internet or mobile apps amount to government control of what people say or do online. These provisions are unconstitutional, contravene international human rights principles, and would cause significant harm.

Allowing the Mexican government to order ISPs to shut down the internet would be unconstitutional. Article 6 of the Mexican Constitution guarantees "access to information and communication technology" without "arbitrary interference," while Article 7 ensures that "[f]reedom of speech, opinion, ideas and information through any means shall not be abridged."[5] Shutting down the internet clearly violates the right to access information because a shutdown would cut access to all information available online. An internet shutdown would also seriously abridge the rights of Mexicans to speak freely, as they would be left without the most important tool for speaking.

Shutdowns would also contravene Article 13 of the American Convention on Human Rights, which specifically addresses situations such as internet shutdowns. Article 13(3) states "[t]he right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the

[4] We further note that the Draft Guidelines provide no clarity on what constitutes a "competent authority."
[5] Constitution of Mexico, Art. 6, "The Federal State shall guarantee access to information and communication technology, access to the services of radio broadcast, telecommunications and broadband Internet. To that end, the Federal State shall establish effective competition conditions for the provision of such services. … B. In matters of broadcasting and telecommunications: … II. Telecommunications are deemed as public services of general interest and, therefore, the Federal State shall guarantee that they are offered under competitive conditions, with quality, plurality, universal coverage, interconnection, convergence, continuity, free access, and free from arbitrary interferences." See also Art. 7, "Freedom of speech, opinion, ideas and information through any means shall not be abridged. Said right shall neither be abridged through any indirect means, such as abuse of official or private control over paper, radio electric frequencies or any other materials or devices used to deliver information, or through any other means or information and communication technologies aimed at impeding transmission or circulation of ideas and opinions. No statute or authority shall establish prior restraints, nor shall it abridge freedom of speech, which shall be subject to no other limitation than those foreseen in the first paragraph of Article 6 of this Constitution. Under no circumstances shall the assets used for the transmission of information, opinions and ideas be subject to seizure on the grounds of being an instrumentality of a felony." Political Constitution of the United Mexican States, https://www.te.gob.mx/sites/default/files/consultas/2012/04/political_constitution_v2_pdf_20009.pdf.

communication and circulation of ideas and opinions."[6] Shutting down the internet constitutes an abuse of government controls that would restrict free expression by impeding communication over the network.

Intentional disruptions to the internet violate international law. The UN Human Rights Council and the UN General Assembly have passed, by consensus, multiple resolutions that unambiguously condemn internet shutdowns and similar restrictions on freedom of expression online.[7]

Further, allowing government shutdowns would go beyond what is already provided for in Mexico's National Security Law and other laws, which do not provide authority to order the censorship of applications, content, or services on the internet.

Government shutdowns cause significant harm to everyone involved, including users, emergency services, journalists, human rights defenders, demonstrators, and businesses. Shutting off what is often people's lifeline, or means to earn a living, causes obvious problems for people who may no longer be able to communicate with family in times of need, operate their business, or find information.

Similarly, internet shutdowns do not help victims or restore order.[8] On the contrary, research suggests that internet shutdowns and violence go hand in hand.[9] A study on internet shutdowns in India, a country consistently with the greatest number of shutdowns each year,[10] suggested that rather than curbing protests and violence, shutdowns fueled unrest as "each successive day of protest had more violence than would typically happen as a protest unfolded with continued internet access."[11] When individuals are disconnected in the midst of protests and

---

[6] American Convention on Human Rights, http://www.hrcr.org/docs/American_Convention/oashr4.html.
[7] See, e.g., UN Human Rights Council in Resolution A/HRC/RES/32/13, https://ccdcoe.org/uploads/2018/11/UN-160701-A_HRC_Res_32_13.pdf (noting the deep concern over "measures aiming to or that intentionally prevent or disrupt access to or dissemination of information online, in violation of international human rights law").
[8] An internet shutdown is defined as an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information. Targeted, Cut Off, and Left in the Dark, Access Now (Feb. 2020), https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf, at 2 ("2019 KeepItOn Report"). See also Anita R. Gohdes, Pulling the Plug: Network Disruptions and Violence in the Syrian Conflict, Journal of Peace Research (Jan. 31, 2014), http://www.anitagohdes.net/uploads/2/7/2/3/27235401/gohdes_synetworkaug14.pdf.
[9] Gohdes, supra note 8.
[10] The State of Internet Shutdowns Around the World, Access Now (July 2019), https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf, at 2 (showing India with 134 shutdowns in 2018); Targeted, Cut Off, and Left in the Dark, Access Now (Feb. 2020), https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf, at 2 (showing India with 121 shutdowns in 2019).
[11] Jan Rydzak, Shutting down social media does not reduce violence, but rather fuels it, PRI News (Apr. 29, 2019), https://www.pri.org/stories/2019-04-29/shutting-down-social-media-does-not-reduce-violence-rather-fuels-it.

unrest, they may be prevented from reaching necessary, emergency services or from accessing life-saving information. These India shutdowns harmed those users without restoring order and consistently put vulnerable populations and civil society at risk.

Internet shutdowns also take an enormous economic toll on societies. A study by the Brookings Center for Technology Innovation estimates that the global costs of shutdowns between June 2015 and June 2016 were over $2.4 billion.[12] An estimated 4.2% of Mexico's GDP is derived from the internet economy.[13] Therefore, an internet shutdown would likely have a significant economic impact on the country.

Government shutdowns are unfortunately common throughout the world. According to the recently-released #KeepItOn report, there were 213 shutdowns in 33 countries in 2019.[14] Latin America saw at least 14 shutdowns in Venezuela and Ecuador. As the global trend moves toward more frequent and sophisticated shutdowns, the responsibility falls on governments to refrain from implementing shutdowns and to ensure that the rights to freedom of expression and access to the internet are properly enshrined in law.

To comply with these international, regional and local laws, sections III and IV of Article 5 of the Draft Guidelines should be removed.

3. The IFT should impose strong Net Neutrality protections and disallow paid prioritization and zero rating.

Net Neutrality is the guiding principle that preserves the free and open internet. This principle assures that ISPs do not discriminate based on the origin, destination, or 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.

Net Neutrality relates to three core principles for the functioning of the internet, enabling and complimenting them: end-to-end connectivity, best effort in traffic delivery, and permissionless innovation. 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 without undue interference. Second, the *best effort* principle guarantees that all traffic intermediaries on the internet should make their best effort to deliver traffic from one point to another as expeditiously and effectively as possible. Finally, the *permissionless innovation* principle states that everyone should be able create products and services without requiring the authorization of other entities, particularly those who exert technical control over basic infrastructure.

---

[12] Darrell M. West, Internet shutdowns cost countries $2.4 billion last year, Center for Technology Innovation at Brookings (Oct. 2016), https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf.
[13] *Id*. at 6.
[14] 2019 KeepItOn Report at 2.

The Draft Guidelines merely recite several broad, high-level principles regarding traffic management and then allow ISPs to implement "differentiated" or "specialized" services. The breadth of the principles and the express allowing of paid priority schemes will undermine Net Neutrality. Adopting the regulations as proposed would lead to the exact problem that Net Neutrality regulations are attempting to prevent, and would further cement ISPs' role as gatekeepers to the internet.

First, the high-level principles in Articles 3 and 4 are insufficient because they are extraordinarily broad and will likely be extremely difficult to enforce. For instance, Article 3(III) allows network management practices to "[e]ncourage commercial innovation," which could be read simply to encourage innovation *by the ISP*. Such a broad reading could allow an ISP to, for instance, implement network slicing in a 5G network (where different services reach customers at different speeds) because ISPs could argue such technology is "innovative," even though network slicing is directly contrary to Net Neutrality.[15] In Article 4(II), ISPs can manage traffic so long as it provides "[n]on-discriminatory treatment to final users," even though paid priority schemes (which undermine this principle) are expressly allowed in Articles 7 and 8.

Second, allowing "differentiated services," including when online companies "sponsor" data consumption and "free" access to content akin to zero rating, could cause serious harm to users' ability to seek the content they desire, and could lead to a distorted online marketplace. Allowing differentiated services grants ISPs the ability to carry out discriminatory traffic management, granting preferential treatment to certain content online to detriment of others, for almost any reason and potentially in return for monetary benefit. Zero rating is a similar practice, except implemented in a way where certain data is exempted from a user's data allowance. Such a practice would incentivize ISPs to preserve and exploit network capacity scarcity to generate interest from providers of applications, content, and services, to pay for the prioritization of their traffic.

Merely requiring equal terms for all specialized services is insufficient. This practice, in general, favors large companies that can more easily justify spending a relatively smaller portion of their revenues on ensuring ISP priority, and would leave smaller competitors with little ability to compete on a level playing field. Large companies would have extensive audiences while smaller companies and nonprofits would fall behind, further cementing the power of large websites and social networks.

The user experience would likely suffer too. With certain services prioritized, users could be nudged or even forced to use the products of larger competitors whose services function better and more efficiently than smaller competitors' services, even if they are inferior products.

For similar reasons, the Draft Guidelines violate the Federal Law on Telecommunications and Broadcasting which enshrines the Net Neutrality principle and its non-discrimination and free

[15] Monica Alleven, FCC's plan to toss net neutrality is a win for 5G: analyst, FierceWireless (Nov. 22, 2017), https://www.fiercewireless.com/wireless/fcc-s-plan-to-toss-net-neutrality-a-win-for-5g-analyst.

choice manifestations in Articles 145 and 146. These Articles require that the IFT ensure that ISPs "refrain from obstructing, interfering, inspecting, filtering or discriminating content, applications or service" and "respecting the capacity, speed and quality contracted by the user, regardless of the content, origin, destination, terminal or application, as well as the services provided through the Internet."[16] If the IFT fails to explicitly prevent blocking, throttling, and paid priority, it would essentially allow ISPs to violate these laws that do not allow ISPs to "interfer[e]" with content.

The Draft Guidelines should be amended to include specific rules against blocking, throttling, paid prioritization, and zero rating to ensure ISPs do not engage in these behaviors.[17] The IFT should also consider monitoring interconnection issues to ensure ISPs do not violate Net Neutrality through interconnection agreements, and consider monitoring ISP behavior through a general conduct standard, as the U.S. Federal Communications Commission imposed in 2015.[18]

4. The IFT should provide robust ISP privacy protections.

The law requires that the IFT impose regulations that protect the privacy of users.[19] However, the Draft Guidelines do not, but should, include privacy protections beyond mere transparency.

Because an ISP provides customers with access to the internet, it has extensive data about those customers. ISPs process an enormous amount of information, much of which is highly personal customer data.[20] ISPs know where their customers live, their contact information, the websites and apps they visit and use, when they use their devices, and various and extensive fine-grained details about their customers. Some may even use "Supercookies," or similar deep packet inspection technology, which are designed to track all browsing data of customers.[21]

---

[16] Federal Telecommunications and Broadcasting Law, Mexican Congress, http://www.ift.org.mx/sites/default/files/contenidogeneral/asuntos-internacionales//federaltelecommunicationsandbroadcastinglawmexico.pdf.

[17] Access Now Comments to U.S. Federal Communications Commission Regarding Net Neutrality Proceeding 17-108 (July 17, 2017), https://www.accessnow.org/cms/assets/uploads/2017/07/Access-Now-NPRM-Comment_July-17-2017.pdf

[18] Report and Order on Remand, Declaratory Ruling, and Order, Promoting the Open Internet (Mar. 12, 2015), https://docs.fcc.gov/public/attachments/FCC-15-24A1.pdf (see ¶31 for interconnection, ¶138 for general conduct).

[19] See Article 145(III) of the Federal Law on Telecommunications and Broadcasting. Federal Telecommunications and Broadcasting Law, Mexican Congress, http://www.ift.org.mx/sites/default/files/contenidogeneral/asuntos-internacionales//federaltelecommunicationsandbroadcastinglawmexico.pdf.

[20] Letter to Marlene H. Dortch, Secretary of the FCC, from Access Now, Re: Protecting the Privacy of Customers of Broadband and Other TelecommunicationsServices, Dkt. No. 16-106, https://www.accessnow.org/cms/assets/uploads/2016/05/NPRM-PrivacyofBroadbandCustomers-_-Access-Now.pdf.

[21] The Rise of Mobile Tracking Headers, Access Now (Aug. 2015), https://www.accessnow.org/cms/assets/uploads/archive/AIBT-Report.pdf.

The transparency proposal regarding privacy practices is insufficient. The Draft Guidelines in Article 13(III) propose to require ISPs to publicize "[r]ecommendations for final users to minimize risks to their communication privacy." However, customers typically do not have a choice between providers and therefore must accept their ISP's privacy practices. Users cannot "vote with their feet" by leaving a provider if they do not like their ISP's privacy practices. Moreover, transparency over privacy practices has failed. The prime example of that is the United States, which has focused on a transparency privacy framework for two decades, and that has led to innumerable privacy violations and data breaches that left users in danger. Last, users can be coerced into giving up their privacy in exchange for a discount or other reward, which will unnecessarily harm at-risk (low-income and marginalized) communities, a practice that should not be allowed.

At the very least, ISPs must be transparent about the following privacy-related practices:

- What information is stored by the company, 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"; and
- What consumer information will be turned over to law enforcement absent any court order.[22]

But even if the IFT were to implement these stronger transparency requirements, the IFT must protect ISP users with strong, substantive privacy protections because ISPs cannot necessarily be trusted to be forthcoming about their practices or act in the best interest of the customer. Recently, the U.S. Federal Communications Commission took enforcement action against the four major U.S. wireless carriers for selling the real-time location data of their customers to, among others, bounty hunters.[23] Further, ISPs can use intrusive practices like deep packet inspection for a variety of purposes, and the IFT should monitor and potentially prevent ISPs from using such technologies if they are found to be too intrusive.

5. **The IFT should require improved ISP network management transparency.**

[22] Access Now Comments to U.S. Federal Communications Commission Regarding Net Neutrality Proceeding 17-108 (July 17, 2017), https://www.accessnow.org/cms/assets/uploads/2017/07/Access-Now-NPRM-Comment_July-17-2017.pdf at 20.

[23] FCC Proposes over $200 Million in Fines Against Four Largest Wireless Carriers for Apparently Failing to Adequately Protect Consumer Location Data, FCC (Feb. 28, 2020), https://docs.fcc.gov/public/attachments/DOC-362754A1.pdf.

The Draft Guidelines should require more network management transparency to better allow internet users and the IFT to evaluate compliance with the ultimate regulation and ensure ISPs respect Net Neutrality.

A critical, though not on its own sufficient, part of protecting Net Neutrality involves ISPs being transparent about their business and network management practices. ISPs must publicly disclose information regarding their network management practices, performance, and commercial terms of service. For example, ISPs should disclose technical details about the user's connection, such as expected performance metrics (speed, latency, packet loss), as well as commercial terms including what types of data are exempted from data allowances (if zero rating is allowed). Further, ISPs should disclose whether connection speeds differ based on length or type of contract, device, location, or connection protocol.

The disclosure requirements in Article 10 should not be limited to ISPs that offer differentiated or specialized services. These requirements must extend to all ISPs and be made available via a publicly available, easily accessible company website or through the IFT's website. This will help discourage harmful practices and help regulators target problematic conduct.

6. Petition / Petitorium

For the reasons expressed above, we urge the IFT to revise and amend the Draft Guidelines to ensure that Net Neutrality and users' rights to an open internet will be protected. We look forward to continuing to engage in this process.

Respectfully,

/s/

Gaspar Pisanu
Latin American Policy Associate
Isedua Oribhabor
U.S. Policy Analyst
Eric Null
U.S. Policy Manager, Global Net Neutrality Lead