April 13, 2020

Gabriel Oswaldo Contreras Saldívar, Presidente
El Instituto Federal de Telecomunicaciones
Insurgentes Sur #1143, Col. Nochebuena,
Demarcación Territorial Benito Juárez, Ciudad de México 03720

RE: Mozilla's comments on Mexico's draft net neutrality guidelines

Dear Sirs,

Thank you for this opportunity to provide comment and input to the Federal Institute of Telecommunications (the Institute) on your Draft Guidelines for Traffic Management and Internet Administration (Draft Guidelines)[1], implementing the net neutrality requirements of the Federal Telecommunications and Broadcasting Law (FLTB)[2]. We welcome this discussion of the appropriate regulatory framework for protecting net neutrality, and support regulatory action to ensure the internet's continued openness.

Mozilla's mission is to ensure the internet is a global public resource, open and accessible to all. As part of these efforts, we have been involved in efforts for strong net neutrality regulation on four continents. Our flagship product is Firefox, which is an openly developed and open source web browser used by hundreds of millions of people worldwide. Mozilla is also a foundation that educates and empowers internet users around the world. Finally, Mozilla is a global community of technologists, thinkers, and builders, including many contributors and developers in Mexico, who work together to keep the internet open and accessible.

Net neutrality is critical to maintaining the continued success of the open internet as an engine for innovation, opportunity, and learning. We stand firm in the belief that all users should be able to experience the full diversity of the Web, and for services to compete on equal footing. It is important that all internet traffic be treated equally, without discrimination against content or type of traffic — that's the how the internet was built and what has made it one of the greatest

[1] Anteproyecto Lineamientos para la gestión de tráfico y administración de la red a que deberán sujetarse los concesionarios y autorizados que presten el servicio de acceso a Internet, http://www.ift.org.mx/sites/default/files/industria/temasrelevantes/13791/documentos/1documentoenconsultapublicaanteproyectodelineamientos.pdf

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

inventions of all time. For this to be possible, Internet Service Providers (ISPs) must treat all content transmitted over the internet equally. Additionally, net neutrality rules must be comprehensive, enforceable, and the Institute must have, and use, enforcement authority to protect users. While these Draft Guidelines are a good beginning for net neutrality protections, they are incomplete and allow for government shutdowns and zero-rating practices - both of which threaten the ability of Mexican users to freely access the internet. While these guidelines form the beginnings of net neutrality protections for Mexicans, there are additional protections that should be included.

In this submission, we will comment on eight aspects of the Draft Guidelines:

- The definition of net neutrality
- Reasonable traffic management practices
- Specialized services
- Zero-rating and discriminatory traffic management practices
- Transparency
- Tools for measuring and detecting net neutrality violations
- Intervention in traffic management
- Privacy protections and DPI

If you have any questions about this submission or if we can provide any additional information, please do not hesitate to contact Heather West, Head of Americas Policy, at heather@mozilla.com.

Definition of net neutrality

The open internet relies on many technological and legal assumptions for its continued vitality. One of those assumptions is net neutrality. Net neutrality is grounded in three principles:

1. The end-to-end principle: All points in the network should be able to connect to all other points in the network;
2. The best efforts principle: ISPs should deliver all Internet traffic from point to point as expeditiously as possible; and
3. The innovation without permission principle: Everyone and anyone should be able to innovate on the Internet without seeking permission from anyone, any entity, or other gatekeeper.

In practice, net neutrality is a requirement that ISPs treat all data on the internet without discrimination, restriction, or interference no matter the sender, receiver, content, website, platform, application, feature, attached equipment, or means of communication, or any types thereof. A strong requirement against discrimination, restriction, and interference is critical, as is strong enforcement from the Institute.

These principles are critical to ensuring the continued openness of the internet and ensuring the internet exists as a level playing field that enables and supports innovation, competition, and opportunity.

The Institute has already rightfully recognized some of the most flagrant ways that ISPs may unreasonably interfere with internet traffic. In order to protect net neutrality in Mexico, these rules should clearly prohibit:

- Blocking of applications, websites or any other content on the internet;
- Slowing or “throttling” internet speeds;
- Preferential treatment of applications, websites, or any other content on the internet;
- Differential pricing or “zero-rating” for data services based on the applications, websites, or other content being accessed by the user; and
- Inspection of the contents of data packets, except to maintain the security of the network or meet other lawful requirements.

Unfortunately, while the Draft Guidelines consider many of these, the protections included are not adequate to ensure net neutrality.

Reasonable traffic management practices

The Draft Guidelines consider traffic management and network administration policies to ensure the quality and speed of the service, the integrity and security of the network. As in the Draft Guidelines, these practices must ensure the free choice of users to access any content, application or service with non-discriminatory treatment.

Traffic management practices should only be considered reasonable when they are utilized for the purposes of technical maintenance of the network (e.g., to block spam, malware, and attacks on the network), or to mitigate the effects of network congestion under suitable circumstances. Unfortunately, these Draft Guidelines provide significant ability for ISPs or governments to choose to degrade traffic for other reasons, which we will examine in later sections.

There are situations, such as technical congestion or a threat to the integrity of the network, that do require particular traffic management practices. Generally speaking, network congestion can occur due to two conditions:

1) As a result of unpredictable, irregular, and/or temporary network overload; or
2) As the result of a ISP's failure to develop sufficient capacity to handle the network load (which would lead to frequent and sustained windows of network congestion).

In this sense, congestion occurs under exceptional circumstances of unpredictable situations, and reasonable traffic management should be permitted to address these situations. However, the concept of reasonable traffic management should and must be strictly limited to circumstances of unpredictable load at irregular times, and must not be used as a cover for systemic underinvestment in network capacity.

Reasonable traffic management practices may include:

- Adequate disclosure to users about traffic management policies and tools to allow them to make informed choices.
- Application-agnostic controls may be used but application-specific control within the "Internet traffic" class may not be permitted.
- Practices like deep packet inspection should not be used for unlawful access to the type and contents of an application in an IP packet.
- Improper (paid or otherwise) prioritisation may not be permitted.

We also commend for your attention the 2016 Net Neutrality Guidelines of the Body of European Regulators for Electronic Communications (BEREC).[3] For example, in order to be considered "reasonable", traffic management under BEREC guidelines would have to be based on objectively different technical Quality of Service (QoS) requirements of specific categories of traffic. Further, according to BEREC, categories of traffic can be defined, for example, by reference to application layer protocol or generic application type, but only to the extent:

1. They objectively require different technical QoS;
2. All applications with equivalent requirements are handled in the same category; and
3. The justification given is relevant to the category of traffic in question.

[3] BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules

Importantly, BEREC also requires that such measures do not monitor specific content (content provided by the end-users themselves, such as text, pictures and video), and that by virtue of non-discrimination, encrypted traffic is treated equally with normal traffic.[4]

Specialized services

The Draft Guidelines provide expansive permission to offer specialized services in Article 8. It's unclear why much of these rules for specialized services are necessary. Often, the contextual problems used to justify their "need" could be remedied through infrastructure investment, with significant benefits for the ecosystem as a whole. The benefits are also highly dependent on the nature of the implementation, and the source of delays associated with the open internet connection.

If the Institute is going to permit specialized services, we would strongly suggest a far more narrowly targeted set of activities, with more attention paid to ensure that specialized services do not cannibalize bandwidth or the quality of open internet access.

Specialized services should be understood as electronic communication services which are distinct from internet access services and provide a specified level of quality of service generally optimized for specific content, applications, services, or some combination thereof. Such optimisation is necessary in order to meet the specific requirements for the specific level of quality. Specialized services are notable in the current context in that they are sometimes justified by ISPs as a mechanism for reducing network congestion; we believe the use of specialized services in this manner should be subject to strict oversight and limitations.

Technically speaking, specialized services can be engineered in (at least) three distinct ways. First, they could be provisioned over distinct physical infrastructure, as separate wires and other hardware. Second, they could be provisioned as channels within the open internet access service, using bandwidth allocated for the internet access service but on a different priority level to achieve the desired quality threshold. Finally, they could be provisioned as channels that use the same physical infrastructure but a separate logical capacity, virtually walled off from the open internet access service.

The first type of service is both physically and logically distinct from internet access services and thus the least problematic to assess in terms of its potential conflicts with the requirement

[4] About BEREC's Net Neutrality Guidelines, https://berec.europa.eu/files/document_register_store/2016/8/NN%20Factsheet.pdf

to treat traffic in a non-discriminatory manner. Our answer will thus set this variety aside from further consideration, and will address the second and third types in greater detail.

Both the second and third types may be desirable for content providers because they allow some traffic to “cut through” congestion or other delays associated with the open internet service. The primary technical improvement is likely to be reduced latency and jitter for the content delivered by the specialized service, “smoothing” out the transmission pathway regardless of “noise” and traffic load associated with the open internet access service; in some circumstances, bandwidth might be improved as well.

As compared to the second variety, the third, logical separation over shared physical infrastructure, offers the same benefits for the ancillary services with fewer potential harms to competition as compared to shared logical channeling. Sharing both the physical and logical infrastructure (the second variety) is functionally comparable to paid prioritisation arrangements over the open Internet access service, something recognised widely as harmful to competition, innovation, and user choice. In this variety, in the same way as paid prioritisation, giving a benefit to one causes practical harm to others (in that the capacity they could use is less than it would be if the specialized service were not actively in use), as well as challenging the user’s expected bandwidth for their open internet access service (as some of that capacity is cannibalised by the specialized service).

In contrast, logical separation (the third variety) isolates and protects the capacity available to the open internet access service. Use of the specialized service should not create congestion nor performance benefits for uses of other content, applications, and services on the open internet. Although the total bandwidth available to the end user for open internet connectivity is less, suitable disclosures can be made up front, and users will be better empowered to choose whether or not they wish to subscribe to specialized services and thereby limit their open internet usage.

Zero-rating and discriminatory traffic management practices

We are concerned to see that the Draft Guidelines permit the use of zero-rating and sponsored data in Article 7. While paid prioritization is frequently invoked as a clear violation of net neutrality, subsidization that makes some content available for free and other content only available at a cost raises similar concerns. As with blocking, throttling, or paid prioritization, this differential pricing can enable ISPs, as gatekeepers, to disrupt the internet’s level playing field. Even with platforms that claim to be open to any site or service that meets certain technical specifications, we are concerned with how open they would be to including a new, startup competitor to their established services and those of their partners.

In 2017, Mozilla commissioned research[5] to investigate how and why people use subsidized services in Myanmar, Peru, Kenya, Nigeria, Rwanda and South Africa. This research, conducted by Research ICT Africa, LIRNEasia and IEP, found that in all countries surveyed, users are not coming online through zero-rated services. While more research is needed, the benefits of zero-rating and differential pricing seem low, while the resulting risk of these offerings creating an anti-competitive environment is extremely high.

This research revealed that people who use zero-rated services usually also have full access to the internet, and make use of zero-rated and subsidized data services as one of many money-saving strategies, including:

- Use of multiple SIM cards to take advantage of promotions, better reception quality, or better prices for a given service.
- Use of public Wi-Fi. For example, many buses in Kenya now provide Wi-Fi access, and participants reported being willing to wait for a bus that was Wi-Fi-enabled.
- Tethering to mobile hotspots. In South Africa and India, users not only share data but also promotions and subsidized offers from one phone to another.
- Earned reward applications (where users download, use, or share a promoted application in return for mobile data/credit). The research indicates that most users tend to play the system to get the most credit possible and then abandon the earned reward application.
- While users, especially in the African studies, report skepticism about whether zero-rated promotions are truly free, partially subsidized bundles are popular.

While zero-rated services tend to be only part of internet usage for most users studied, some users are getting trapped in the walled gardens of these subsidized offerings.

- In particular, low income respondents in Peru and Rwanda use zero-rated content for much of their browsing activity, as do rural respondents in Myanmar.
- Awareness matters: in Myanmar, respondents who know they are in a zero-rated walled garden (e.g., due to lack of photos and video) are more likely to access the full internet beyond the walled garden.
- But, when Facebook is subsidized without impacting user experience, users tend to concentrate their usage on that single site, demonstrating concerns around the anti-competitive effects of zero-rating.

[5] Mozilla releases research results: Zero rating is not serving as an on-ramp to the internet, https://blog.mozilla.org/blog/2017/07/31/mozilla-releases-research-results-zero-rating-not-serving-ramp-internet/

Equal Rating as an alternative

In the belief that there can and must be business models that will serve to connect the unconnected, and connect them to the full diversity of the open internet without violating the principles of net neutrality, Mozilla has pioneered the concept of "equal rating". Building on Mozilla's strong commitment to net neutrality, equal rating models are free of discrimination, gatekeepers, and pay-to-play schemes. Equal rating stands in contrast to zero-rating business models, which reduce the cost to zero only for some sites and services. Our Equal Rating Innovation Challenge,[6] which received hundreds of submissions from more than 25 countries, demonstrates the many ways that companies and entrepreneurs are making the internet affordable and accessible around the world. We suggest consideration of equal rating rather than zero-rating.

Transparency

Transparency is key to ensuring compliance with any net neutrality regulation. Unfortunately, this topic gets too little attention in the Draft Guidelines. In particular, we recommend transparency around the following practices:

1) Price information and commercial terms,
2) Performance characteristics,
3) Traffic management practices,
4) Specialized services, and their impact on internet access services.

Net neutrality violations can occur in many different ways and at different points in the network, hence the need for a holistic monitoring as well as transparency regime. We respectfully recommend that the Institute require disclosures to the end user on the aforementioned categories of information at the point of sale. Given that ISPs' practices and capacity will likely change over time, additional disclosures of each of these categories of information should be made to the end user on an at least annual basis, and whenever there is a substantial change. These disclosures to the end user should be required to be provided in a clear, comprehensive, and accessible form. Without adequate disclosure to the public, users cannot make informed choices about the services they wish to purchase.

We would also suggest that the Institute require notification to users when their individual use of a network will trigger a traffic management practice that is likely to have a significant impact on their experience of the internet. Such disclosures are important to help users understand any

[6] Announcing the Equal Rating Innovation Challenge Winners, https://blog.mozilla.org/blog/2017/03/29/announcing-equal-rating-innovation-challenge-winners/

network interference they are experiencing and to modify their behavior accordingly, including potentially purchasing alternative services.

In order for the Institute to carry out its mandate and to appropriately oversee compliance with net neutrality regulation, we also recommend requiring detailed disclosures by ISPs to the regulator on price information and terms, performance characteristics, traffic management practices, and specialized services on an at least annual basis, as well as requiring additional disclosures when there is a substantial change in practices or offerings.

Disclosure of technical information about traffic management practices could prove invaluable for other service providers seeking to optimize their applications and services. For example, an ISP's available APIs, precise traffic performance metrics, and location and capabilities of network infrastructure -- the sort of information routinely exchanged with business partners -- would provide value to businesses seeking to reach end users over a ISP's network, yet may not make sense for inclusion in a primarily user-facing template. We encourage the Institute to consider the possibility of enhanced disclosure to promote competition and innovation to the fullest degree.

The Institute may furthermore benefit from additional information provided by ISPs in the enforcement of future policies. For example, as regards traffic management practices (TMPs), we would recommend the Institute require disclosures on how technically traffic management is accomplished, what classes if any were used to engage in traffic management, how often TMPs were used, and other, similar information to allow the Institute to understand generally how TMPs are being deployed in evolving network environments.

The Institute will likely be interested particularly in specialized services, including information such as whether the specialized service is provisioned over separate physical and/or logical infrastructure, information about how specialized services are affecting internet service offerings, and the details of commercial partners involved in any specialized services.

Effective enforcement of net neutrality requires both quantitative and qualitative approaches to document consumer experiences. Therefore, allowing consumers and other interested stakeholders to submit qualitative descriptions of experiences while also simultaneously creating detailed technical descriptions and formats for submitting such data would enhance effective monitoring of ISP practices at scale. The qualitative descriptions alone, when not accompanied by the quantitative technical description, could then be used to further investigate that particular provider and geographical region by the Institute using technical tools (see next section).

Finally, BEREC's Net Neutrality Regulatory Assessment Methodology[7] lists out technical specifications categorised into speed measurements, delay and delay variation measurements, and packet loss measurements categories that can serve as a framework for the detailed technical description that should be required by the Institute.

Tools for measuring and detecting net neutrality violations

In order to aid technical measurement of net neutrality violations, the Institute could follow the model of BEREC, which commissioned the creation of a Net Neutrality Measurement Tool that combines multi-modal means of measurements of network parameters that collectively can be used to determine violations of net neutrality. The specification sheet[8] for the tool could be the model for a similar project in Mexico, or even serve as the direct foundation for the codebase for a Mexican tool as a collaborative effort with BEREC since the tool itself will be open source when released. The specification sheet also contains a good technical underpinning (Section 3.1) for the various parameters that can be used to detect violations of net neutrality such as speed measurement, delay measurements, application specific measurement, and additional modules.

Once available, the Institute can:

- Run the tool regularly from its offices which are spread around the country; and
- Mandate that ISPs run the tool on a regular basis; and
- Mandate that ISPs upload the results of running the tool as a part of their public disclosures; and
- Spread public awareness across the country of crowdsourcing tools to interested members of the public.

The Open Observatory of Network Interference (OONI)[9] and M-Lab[10] projects are good models on how to encourage and leverage public monitoring of network neutrality. The Institute can also look to these projects to inform their technical standards and deployment best practices.

[7] BEREC Net Neutrality Regulatory Assessment Methodology, https://www.berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/methodologies/7295-berec-net-neutrality-regulatory-assessment-methodology

[8] Net neutrality measurement tool specification, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/7296-net-neutrality-measurement-tool-specification

[9] OOMI: Open Observatory of Network Interference, https://ooni.org/

[10] M-Lab, https://www.measurementlab.net/

Intervention in traffic management

We are deeply concerned by the expansive powers granted to the Institute, and potentially other parts of the Mexican government, in Article 5. Specifically, giving ISPs the ability to "implement traffic management and network administration policies that result in the limitation, degradation, restriction, discrimination, obstruction, interference, filtering or blocking of access to content, applications or services to final users… **at the express request of the competent authority**" or in an "**emergency or national security situations as provided by law**" (emphasis added) provides broad ability for government entities to interfere with the provision of internet services.

While some amount of traffic management is at times needed for the proper management of network resources and to mitigate security threats, this is best handled by ISPs themselves, subject to appropriate regulatory oversight. We do not see any legitimate situation where it would be appropriate for the Institute or another part of the government to exercise such powers. The ability to limit, degrade, restrict, discriminate, obstruct, interfere, filter, or block access to content, applications, and services could easily be abused as a means of censorship and surveillance. These powers could also be used to effect an internet shutdown. These types of network interference pose a substantial threat to free expression and the ability of users to freely seek, receive, and impart information.

The internet is a global public resource that must be open and accessible to all, the second principle in the Mozilla Manifesto[11]. Shutdowns and network interference cause real harm to users, no matter where they occur. In times of emergency, users need more, not less information. Cutting off information only increases disorder, and can deny people in need from getting urgently needed help and contacting their friends and loved ones. The best way to protect Mexican users is to ensure that the internet remains accessible at all times. As such, we urge you to remove these two clauses from the final version of Mexico's net neutrality regulations.

[11] The Mozilla Manifesto, In Spanish: https://www.mozilla.org/es-ES/about/manifesto/ ; In English: https://www.mozilla.org/en-US/about/manifesto/details/

Privacy protections and Deep Packet Inspection

While privacy is one of the key principles of a net neutrality regulation required by the FTBL in Chapter VI, Article 145[12], we are surprised and alarmed to see only a passing mention in Article 3, rather than a robust set of privacy protections in these Draft Guidelines. The Institute should develop guidance on how ISPs must protect user data, as the FTBL states. This protection should extend to both the data associated with their account, as well as the use of their services by their customers.

Notably, the regulation should address the use of Deep Packet Inspection (DPI), which is often described as a traffic management technique but has significant privacy implications. DPI is a method of examining the data in packets sent over the network, and can be used to filter or block particular kinds of traffic.

With regard to DPI, we note that reasonable network management as employed in practice today utilizes networking equipment that looks beyond packet header information in the ordinary course of its operation. However, the legitimate use of deep packet inspection technology for reasonable traffic management should not be used to violate or compromise the privacy of internet users.

Conclusion

Mozilla's mission is to ensure the internet is a global public resource, open and accessible to all. Net neutrality rules as envisioned by the FTBL are a critical component of keeping the internet open and accessible, and to continuing the success of the innovation, opportunity, and learning afforded by the open internet.

The Institute should strengthen the Draft Guidelines in order to ensure that ISPs do not unnecessarily interfere with the traffic requested by their customers. Any net neutrality rule that protects Mexicans will require a strong definition of net neutrality that is protected through an empowered regulator, who is protecting users and ensuring that ISPs are acting fairly.

- The Draft Guidelines should be modified to have a more limited set of acceptable traffic management techniques, and the inclusion of specialized services should be reconsidered.

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

- The Draft Guidelines should not permit expansive zero-rating, but rather consider equal-rating as an alternative to provide choices to users that do not run afoul of net neutrality principles. This would be significantly more in line with the guidelines in the FTBL.
- The Draft Guidelines should be modified to more strongly define a limited set of traffic management techniques and the circumstances they may be used under - limiting it to exceptional circumstances that threaten the network. Additionally, the draft should have a much more limited set of specialized services that are permitted.
- The Draft Guidelines should clearly outline the kinds of disclosures required of ISPs to their customers and the Institute. Additionally, the Institute should require the use of measurement tools to detect net neutrality violations.

Again, if you have any questions about this submission or if we can provide any additional information, please do not hesitate to contact Heather West, Head of Americas Policy, at heather@mozilla.com.

Thank you for the opportunity to engage in this process.

Respectfully,

Heather West
Head of Americas Policy
Mozilla, Co.
heather@mozilla.com