



Comments of the Wikimedia Foundation and Wikimedia México on the Anteproyecto de Lineamientos para la gestión de tráfico y administración de red a que deberán sujetarse los concesionarios y autorizados que presten el servicio de acceso a Internet

March 3, 2020

The Wikimedia Foundation and Wikimedia México thank the Instituto Federal de Telecomunicaciones (IFT) for the opportunity to submit these comments on the *Anteproyecto de Lineamientos para la gestión de tráfico y administración de red a que deberán sujetarse los concesionarios y autorizados que presten el servicio de acceso a Internet*. As organizations whose missions require that people around the world have reliable, non-discriminatory access to the Internet, we appreciate the Institute's moving forward on this important issue. However, we have substantial concerns with certain aspects of the draft guidelines that could undermine their stated objectives of promoting free choice, protecting transparency, and its key mission of preventing discrimination.

Background

The Wikimedia Foundation is the international non-profit organization that hosts and supports numerous free and open knowledge educational and informational resources, including Wikipedia. Its mission is to empower and encourage people around the world to gather and develop educational content under a free license or in the public domain, and to disseminate it effectively and globally. Wikimedia México is a non-profit civil association and an independent chapter of the Wikimedia Foundation in Mexico. Its purpose is to spread and promote Wikipedia and the Foundation's projects in Mexico.

Wikipedia, Wikimedia Commons, and all of the various Wikimedia projects are offered to the public for free. The projects are not sponsored by advertising, and rely solely upon donations — not only of money, but also of the time and effort that volunteers put into creating the content that the

Imagine a world in which every single human being can freely share in the sum of all knowledge.

world can view on our websites. Spanish-language Wikipedia, for example, receives 170 million unique visitors per year, who come to read any of its 1.6 million articles.¹ All of those articles and edits are created by the more than 16,000 editors who edit the site every four seconds, sharing their knowledge with the world.² There is no central editorial board for the contents of Wikipedia: anyone with an Internet connection can edit it. The open nature of this writing and editing process serves to democratize knowledge, resulting in a shared knowledge resource of surprising accuracy.

Wikipedia and its fellow projects rely upon the ability of their thousands of editors, and millions of readers, to reach the same website, where each of them can communicate with each other. And each of these users depends upon some Internet service provider (ISP) to reach that same site.

That dependency places the ISP in a position of critical power, with the ability to act as a gatekeeper for users' access to different websites, by assigning a higher priority to certain sites, or certain types of communication, or by blocking traffic to certain sites altogether. While this power can be used for legitimate network security and traffic management purposes, it can also easily be used to favor the business interests of the ISP in ways that discriminate against various groups and competitors. Unfortunately, the line between legitimate management and anticompetitive abuse is often poorly defined, making it easy for ISPs to deliberately or accidentally enact discriminatory policies under the authority of legitimate traffic management.

Because Wikimedia projects are not funded through advertising, and because the non-profit Foundation does not pay ISPs or telecommunications carriers for preferential carriage, policies that create incentives for ISPs to favor the traffic of certain content providers over others will disadvantage our sites and users, whether they seek to share their knowledge or learn from others.

Overbroad Authorization for Traffic Management

Chapter II of the draft guidelines begins by stating that traffic management and network administration policies are justified if they ensure quality and speed; preserve network integrity and safety; and promote business innovation. This opening may serve as a statement of general intent, but

¹ <https://es.wikipedia.org/wiki/Especial:Estad%C3%ADsticas>;
<https://stats.wikimedia.org/#/es.wikipedia.org>.

²*Id.*

its provisions are so open-ended that it may encourage practices that functionally violate the principles of net neutrality and nondiscrimination.

ISPs are naturally inclined to ensure quality and speed, and their interests are largely aligned with their customers' in doing so in the most general sense. However, traffic management practices that allow certain applications and services to maintain a high quality of service by degrading other offerings create an incentive for ISPs to underinvest in infrastructure, providing sustained quality only for the most profitable or popular services.

Furthermore, the precise definitions and applications of quality of service can hide discriminatory conduct. For instance, even if most users would acknowledge that certain types of online applications, like video conference calls, are more sensitive to latency than other applications, such as downloading large files or movie streaming, ISPs can devise quality of service categorizations that may appear facially neutral but still discriminate against competitors. An ISP that classified all video services as requiring a higher level of priority could be discriminating against a videoconferencing application that competed with the ISP's traditional voice offerings, or any video telephony offerings. By including the competitor's services in the same priority tier as a multitude of movie streaming and other audiovisual services, the ISP could increase congestion for the latency-sensitive competitor while offering its own services separately either via traditional telephony or as separate service with dedicated bandwidth.³ Effective rules preventing similar practices should be in place, with clear standards that ensure that quality and speed cannot authorize practices that lead to discriminatory results.

As for the third criterion listed in Article 4, "business innovation" is a term that can be interpreted so broadly as to encompass nearly any practice. This can include practices that harm consumers and violate human rights. While innovation is a laudable goal, it alone cannot justify practices that should otherwise be prohibited. For example, various types of price discrimination are business innovations that can prevent economic inefficiencies, but price discrimination along the lines

³ ISPs should not be allowed to avoid scrutiny of anticompetitive practices on the Internet simply because they are engaged in intermodal competition. An ISP should not be allowed to discriminate against an Internet voice application in order to favor its own traditional voice offerings, even if those offerings are not considered a "specialized service."

of ethnicity, gender, religion, or other categories would often be illegal. Similarly, price discrimination that results in anticompetitive behavior, or interferes with end users' privacy and rights of free expression should not be permitted. "Business innovation" can be used to encompass practices that are purely in the interest of aligned businesses, such as a specific ISP and an allied application provider. In such cases, the only innovation is frequently an innovation in business practices that benefit only those parties, and not consumers, market efficiency, or the public interest.

Too often, profitable but inequitable business practices are justified as increasing potential infrastructure investment, based upon the bare assertion that increased ISP revenues from price discrimination will naturally lead to increased investment. However, there is little evidence to support this.⁴ Especially where consumers have a limited numbers of choices, where switching costs are high, or where small numbers of competitors can easily pursue similar courses of action, ISPs can easily be incentivized to spend revenues gained through paid prioritization or other discriminatory practices on things other than costly infrastructure (such as marketing, cross-promotions, or stock buy-backs), or simply hold those revenues in reserve.

Similarly, ISPs may be tempted to blame congestion on the most popular content, services, or applications available. However, this should not place ISPs or regulators in the position of effectively exercising central price controls for online content. If end users display high demand for particular sites or applications, they should not be punished with higher prices for expressing that demand. Allowing an ISP to set the price on content or services gives it the power to decide the conditions for participation in the online market, which is in itself problematic for free commerce, but also creates clear incentive for discrimination. While such differential pricing may create new business opportunities for an ISP, those opportunities come at a real cost to every other participant in the market.

⁴ See, e.g., Jon Brodtkin, "Title II hasn't hurt network investment, according to the ISPs themselves," *Ars Technica*, May 16, 2017, <https://arstechnica.com/information-technology/2017/05/title-ii-hasnt-hurt-network-investment-according-to-the-isps-themselves/>; Karl Bode, "AT&T, Comcast Dramatically Cut Network Spending Despite Net Neutrality Repeal," *Techdirt*, September 30, 2019, <https://www.techdirt.com/articles/20200129/06135343820/att-comcast-dramatically-cut-network-spending-despite-net-neutrality-repeal.shtml>.

Article 3 should therefore be clarified to ensure that broad statements of business innovation and quality of service cannot be used as a pretext or a justification for practices that disparately affect competitors or degrade or block access to content, applications, or services unfairly.

Vague and Overbroad Permission for Blocking and Throttling

Article 5 could be interpreted to permit nearly every type of service degradation, throttling, or blocking under certain enumerated conditions. Unfortunately, at least two of those conditions are vague and overly broad, permitting blocking, throttling, and degradation of traffic in far too many scenarios.

Article 5.IV permits blocking, throttling, or degrading of traffic “a petición expresa de autoridad competente.” However, the draft guidelines do not specify the scope of competent authorities, leaving open the possibility for requests, from any of a variety of entities and agencies, that may fail to meet basic standards for due process. ISPs should not have to judge how to verify the identity of a local police officer, or make the determination of whether that officer might have competent authority to order the blocking of any given online traffic. Nor should users of the network be subject to the same uncertainty regarding the reliability of their services.

Article 5.V further permits blocking, throttling, or other degradation of traffic “a petición expresa del usuario final.” While consumers may have the ability to request certain types of restrictions, such as parental controls, this broad and general phrasing may still permit ISPs to enact discriminatory practices under the guise of consumer choice.

Online services commonly present requests for consumer consent in deceptive, misleading, or coercive ways, sometimes called “dark patterns.”⁵ Consumers are frequently bombarded by requests for permission from various providers.⁶ These requests are often designed specifically to interrupt users

⁵ See, e.g., Mathur, Acar, *et al.*, “Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites,” *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 81 (November 2019), <https://webtransparency.cs.princeton.edu/dark-patterns/>; “The Illusion of choice and the need for default privacy protection,” *Mozilla*, October 22, 2019, <https://blog.mozilla.org/press/2019/10/the-illusion-of-choice-and-the-need-for-default-privacy-protection/>; Nouwens, Liccardi, *et al.*, “Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence,” <https://webtransparency.cs.princeton.edu/dark-patterns/>.

⁶ Cf. Aleecia M. MacDonald and Lorrie Faith Cranor, “The Cost of Reading Privacy Policies,” *I/S: A Journal of Law and Policy for the Information Society*, 2008 Privacy Year in Review issue, available at

at key points of their interaction, limiting the amount of time users have to evaluate the choice being presented. Frequently, these choices are offered in technical language or marketing jargon, and are designed to deny the user completion of their tasks unless they agree to the terms and conditions offered. Beyond this, consumers are often offered “choices” that are set by default to a particularly favored outcome, technically giving consumers the chance to change the predetermined setting, but allowing consumers who do not carefully inspect the sign-up process to fall into it. Other forms of coercion can come in the form of which services are offered. A communications provider could offer a specialized or differentiated service as the only choice, or the only financially feasible choice, for access, and to avoid the constraints of the draft guidelines, simply refrain from advertising it as a “servicio de acceso a Internet,” instead calling it “online access” or some other newly-developed marketing term.

An ISP hoping to encourage adoption of its preferred prioritization package could present consumers with choices in any of these manners to coerce consumer agreement. The rules should therefore explicitly require that user requests for blocking or degradation actually be desired by users, and not imposed upon them by fine print, default opt-out settings, or coercive pricing schemes.

Finally, the draft guidelines in Article 5 require ISPs to provide the tools and support necessary for consumers to permanently block applications, services, or content. ISPs should also be required to allow consumers to reinstate such applications, services, or content as easily as they can block them. Consumers who are given only a one-way choice are not being given a fully free and open set of choices.

The draft guidelines should therefore narrow the permitted reasons for blocking or throttling, and should prohibit tactics that rely upon deception, coercion, or consumer inattention for obtaining consent. Such practices are in tension with the stated goals of Article 4 of the draft guidelines, as well as Articles 145 and 146 of the Ley Federal de Telecomunicaciones y Radiodifusión Federal (LFTR).

Paid Prioritization

https://kb.osu.edu/bitstream/handle/1811/72839/ISILP_V4N3_543.pdf (finding that, if the average resident of the United States read every privacy policy with which they were presented once a year, the resultant loss of time would cost the United States approximately US\$781 billion).

However, perhaps the most notable issues with the draft guidelines have to do with their language surrounding differentiated and specialized services. We wish to register our deep concern that these portions of the draft guidelines appear to permit paid prioritization of content, applications, or services. Paid prioritization is perhaps the quintessential example of net neutrality violations, being far more commercially viable for an ISP than simple blocking of disfavored content.

Permitting sponsored content effectively narrows the scope of online access, frustrating the benefits of a free and open Internet. Internet users benefit not only from content served by large corporations, but also from non-profit projects and their individual fellow users. Wikipedia is one such example of a non-profit content provider that can easily be crowded out of an online experience where only the highest bidders have access to an audience.

Merely requiring that sponsored content plans be offered on the same terms to all fails to remedy the anticompetitive nature of such agreements. Part of the freedom of expression permitted by the Internet is the ability of rich and poor alike to reach others online. A sponsored data plan that allows financially constrained users access only to content from content providers with the most negotiating power, typically those with the most money. This would leave free projects like Wikipedia out of the hands of those who could benefit from such free online resources. Even if an ISP offered sponsored data plans to every potential content provider at the same rate, any such rate would necessarily exclude from this tier of end users those content providers (including non-profits, small businesses, or individual creators) who cannot afford such fees, leaving the content providers with a smaller market, and the users of such services with an impoverished online universe.

Article 8's requirement that ISPs cannot use the concept of specialized services to demand payment for standard traffic conditions is a worthwhile attempt to forestall an anticipated evasion of competition rules. However, it does not define "condiciones estándar," and thus fails to account for how ISPs may allocate bandwidth between true Internet services and specialized services. If promises of revenues funding additional infrastructure are to be believed, a provider offering a system of specialized services, even with the requirements of Article 8, could have little incentive to allocate bandwidth on its improved infrastructure to open Internet provision. Instead, the ISP could keep bandwidth for a competitive, open Internet frozen at speeds considered standard by the

expectations of 2020, while improving its speeds on less open services. As a result, increased demands for bandwidth would only be met with increasing bandwidth for specialized services, disadvantaging the open Internet. While such practices could be innovative for the revenue streams of an ISP, they would likely slow and constrain innovation in applications or services that are not owned by, affiliated with, or in contract with the ISPs.

Offering other specialized services, such as CDNs or VPNs, is less likely to result in degradation of other users' traffic. However, ISPs that offer such services may still leverage their networks in an anticompetitive manner against parties other than the end user. For instance, even if an ISP offered VPN or CDN service to all customers at the same price, it may be able to use its market position as an ISP to engage in enhance predatory pricing that undercuts non-ISP VPN or CDN providers.

As with allowing consumers to “choose” blocking or throttling, consumers cannot be said to be choosing to agree to contracts regarding zero-rated offerings where their choices are constrained. Consumers with limited purchasing power may have no choice but to accept sponsored data plans, and this choice can be forced if ISPs further promote such plans by limiting plan choices, increasing relative prices overall, or coercively claiming “consent” by using dark patterns to manipulate consumer activity.

As much as the draft guidelines attempt to curb anticompetitive practices associated with specialized and differentiated services, their provisions still permit ISPs to unfairly leverage their gatekeeper role in a two-sided market. This is, in large part, because allowing paid prioritization within the framework of specialized and differentiated services is inherently at odds with the aims of Articles 145 and 146 of the LFTR requiring free choice, non-discrimination, and free competition.

Exclusivity Agreements

The Documento de Preguntas Abiertas asks for comments on the advantages and disadvantages of exclusivity agreements. Exclusivity of content is contrary to net neutrality and constrains consumer free choice. As a basic matter, business arrangements that prevent customers of

one communications service from accessing certain types of content are inherently counter to consumer freedom and free choice.

The Federal Trade Commission guide cited by IFT in support of the idea that exclusive deals are not *per se* anticompetitive specifically does not include cases where the firm using exclusive contracts is a monopolist.⁷ In fact, the FTC guidance calls for further scrutiny when one of the contracting firms is a monopolist. Even aside from concentration in the market for Internet access provision, the ISP is in the nature of a monopolist with respect to access to any given user: the two-sided nature of the market is markedly distant from the simpler example given by the FTC. Exclusivities regarding content are further complicated by the fact that they are frequently dealing with copyrighted content. In this case, the supplier of the copyrighted content is also a form of a monopolist, since copyright law purposefully grants rightsholders exclusivity over the use of their works, and the ability to enforce further exclusive uses by their licensees.

Exclusive deals provide very little incentive for innovative content; more often, they are used to drive consumers to select a provider whose service may otherwise fail to compete on price or traffic quality. In this way, they frequently create disincentives for infrastructure investment, as well as forcing consumers into inefficient tradeoffs that they would otherwise not face.

The justifications frequently offered for exclusive deals thus fail to overcome the initial fact that they represent a restriction on access to content, and are *prima facie* discriminatory towards content.

Transparency Should Include Public Disclosure

⁷ Federal Trade Commission, Exclusive Supply or Purchase Agreements, <https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/single-firm-conduct/exclusiv-e-supply-or> (“However, when the firm using exclusive contracts is a monopolist, the focus shifts to whether those contracts impede efforts of new firms to break into the market or of smaller existing firms to expand their presence. The monopolist might try to impede the entry or expansion of new competitors because that competition would erode its market position. The antitrust laws condemn certain actions of a monopolist that keep rivals out of the market or prevent new products from reaching consumers.”).

The draft guidelines include several provisions for transparency. However, these requirements should require specific disclosures of differentiated and specialized services before they are offered, and these detailed descriptions should be openly published.

For instance, the reports required by Article 11 and the business agreements submitted in Article 12 should be available for public view on their websites, so that consumers and content and application providers may understand exactly how their services and traffic will be affected under various plans, and to understand the nature of the agreements that motivate those choices. Such transparency provides additional safeguards against anticompetitive behavior. The published reports required by Article 11 should also be updated as they change, as opposed to every 3 months.

The code of traffic management policies required in Article 13, likewise, should be sufficiently detailed as to permit each side of the two-sided market (*i.e.*, consumers and content providers) to determine, with reasonable certainty, how their traffic will be affected under given network conditions.

The requirement that the guidelines include recommendations for end users regarding protection of privacy is potentially confusing. If the purpose of the guidelines is to describe the methods of traffic and network management, advice to consumers on privacy and network integrity seem beside the point. Instead, such a requirement can be used to shift responsibility for protecting consumers' privacy and security away from the responsible party of the ISP and onto consumers who are less well-equipped to secure networks that by necessity carry their private information.

Furthermore, in addition to the Institute's periodic review of the guidelines, the Institute should create a process for review of the guidelines upon petition by members of the public, to accommodate disputes resulting from them outside of the three-year cycle.

Finally, we note that Article 9 of the draft guidelines requires ISPs to encourage the development of investment programs aimed at improving infrastructure based on income arising from the provision of differentiated and specialized services. If the rationale for these services is indeed increased infrastructure development, transparency reports should include a detailed accounting of

the revenues accrued from these services, and the specific types and amounts of infrastructure investment on which they were subsequently spent.

Conclusion

The Wikimedia Foundation and Wikimedia México urge the Institute to ensure that its rules fulfill the statutory requirements of Articles 145 and 146 of the LFTR that they prevent discrimination, allowing free choice for consumers, free competition for content providers, and permit the Internet to be the conduit for freedom of expression that it promises to be. To do so, the rules must narrow or eliminate several exceptions, promote *de facto* (and not merely *de jure*) consumer choice, increase mechanisms for transparency, and prohibit paid prioritization.