RESPONSE TO FCC CONSULTATION

Notice of Proposed Rulemaking on
Protecting and Promoting the Open Internet
GN Docket No. 14-28

Introduction

European Digital Rights (EDRi) is an association of 36 digital civil rights organisations from 21 European countries. We welcome the opportunity to provide our feedback to the Federal Communications Commission on the globally important issue of maintaining the free and open internet, to ensure that the core values of the network can be maintained, protecting its current and future generations the social and economic value for this and future generations.

Net Neutrality – what is at stake?

Despite the technical complexity of many of the issues surrounding this subject, the basic principles are quite simple. We start from the (now under threat) legacy position that the internet is an open network, where any end point can connect to any other end point, without permission and without discrimination, on a "best effort" principle. It is this basic value that differentiates the internet from traditional telephony and other communications networks, such as Minitel, which are and were under control of telecommunications operators.

This openness[1] generated – and continues to generate – huge incentives for innovation. Without needing to ask for permission, an activist has access to a world of potential

1No discrimination on the basis of origin, destination, content or technology

supporters and an innovator has access to a world of potential customers. This innovation has created new markets for telecommunications operators – ever-increasing demands for bandwidth has led to increasing incentives for investment and growth.

Net neutrality is a core issue for European Digital Rights because, despite being generally privately owned, the Internet is unquestionably a public space, creating rights and obligations for the enterprises that offer services to and through it. This public space is a new vehicle for achieving and enhancing the freedoms that are recognised by international law and domestic constitutions, including that of the United States. A society that values liberty, democracy and freedom of communication must use all the tools at its disposal to defend these freedoms in the digital age.

An end to net neutrality in the USA will come at severe costs to innovation and competition, privacy and freedom of communication. In this short paper, we would like to briefly assess each of these costs, explaining their origin and consequences.

Economic framework

Despite net neutrality being an issue of major social importance, the aim of those who seek to undermine this principle needs to be clearly understood.

Sending party pays

In essence, large telecommunications operators want to have the right to create a new monopoly – the right to allow or deny access to their customers. Regardless of the mechanisms used to implement such a monopoly (discriminatory peering agreements, discriminatory pricing, blocking/throttling of services or protocols or discriminatory promotion of certain services), this is always the end-goal.

We know from the mobile telephony termination market, that a "sending party pays" (or "calling party network pays") model is extremely resistant to competitive effects, because the injured parties are not the customers of the operator. Instead, it is the companies or services that seek to gain access to the customers of the operator that are disadvantaged – and that generally have limited or no leverage over the access provider. It was for this reason that a situation developed in Europe where, in 2007, the European business telecoms users group INTUG estimated that European consumers were paying 10 billion Euro in "spurious termination fees" in 2007 and legislation was necessary to resolve the problem.[2]

A new music streaming service, for example, may find it impossible to get into the market, because it cannot pay to gain access to the customers of certain internet access providers. However, this will be highly unlikely to be enough persuade a significant number of customers of those access providers to switch services, as long as they have access to (an established) streaming service. This essentially "freezes" the market and creates major barriers to market entry, while reducing incentives to invest in infrastructure.

Conclusion 1: Due to the resistance of sending party pays / calling party network pays markets to competitive influences, the opportunity for consumers to switch operators is of minimal impact on counterbalancing the drive to non-neutral networks.

The European Telecommunications Network Operators (ETNO) association confirmed that it wants to impose sending party pays "in appropriate circumstances" in its submission to the ITU's WCIT conference.[3] The market problems already caused by this model was neatly summarised by J. Scott Marcus[4]: "This CPNP [calling party network pays] system tends to create perverse economic incentives. Carriers tend to be motivated to set termination rates

2 http://intug.org/2008/06/europeans-pay-over-e10-billion-a-year-in-spurious-mtrs/

3 See https://www.etno.eu/datas/itu-matters/etno-ip-interconnection.pdf

4 J. Scott Marcus, Call Termination Fees: The U.S. In a global perspective. Available from ftp://ftp.zew.de/pub/zew-docs/div/IKT04/Paper_Marcus_Parallel_Session.pdf

vastly in excess of real costs, because in doing so they raise, not their own costs, but rather the costs of their rivals".

Specialised services

The "sending party pays" model can either be imposed explicitly (imposing a "toll" on incoming traffic, in the literal "sending party pays" approach), or by following a more circuitous route. One of these methods is to reclassify the services that wish to pay for positive discrimination as "specialised services". Network providers offer access to various services that are not – and cannot be – using specific quality of service guarantees. Certain telemedicine applications are a good example of this. Such services cannot be and should not be offered on the public "best effort" internet. However, a weak legal framework – or simply a weak definition of specialised services – would allow services offered on the public internet to gain an unfair competitive advantage by paying the internet access provider (or, through manipulation) or being forced to do so.

Conclusion 2: Any definition of "specialised services" must be robust enough to prevent a "back-door" undermining of net neutrality. Due to the ever-changing nature of the online market, it may be preferable to focus on non-discrimination principles, as long as these can be enforced quickly and effectively.

Price discrimination

Under the old monopolies, certain services (such as line rental or local calls) were subsidised by others (such as expensive long-distance). Even though this was difficult, it was (and is) widely recognised that services whose prices are not cost-based are unsustainable in a competitive market. A process of tariff-rebalancing is therefore seen as crucial in market liberalisation.

In the mobile internet access market, we see a drift towards anti-competitive cross-subsidies. Operators offer a certain volume of download per month to their subscribers, with additional downloads being paid for on a volume basis. However, certain online

services are either offered (for the moment) or pay for the right to be available "for free", outside the metered service. In the same way as free line rental or free local calls could be seen as societally beneficial, "free" access to certain online services superficially appear to be of some value. However, this market model creates a severe barrier to new online services (or social or political online resources) and, here again, allows the access provider to establish itself as a gatekeeper to a monopoly that is access TO its customer base. If anything, this approach creates more distortions than an unbalanced fixed telephony market. Consequently, such offers are not compatible with an open, competitive, innovation-driven internet environment.

Conclusion 3: Out of bundle "free services" are fundamentally anathema to an open, competitive, innovative online market.

Traffic management

Rules requiring net neutrality would not remove the right of internet access providers to manage their networks in ways that are efficient and protective of the interests of their users.

There are only three limitations that need to be placed on traffic management. It should be done in a way that is technologically neutral, it should be done in a way that is the least privacy-invasive solution that can reasonably be implemented and it should only be used to deal with transient, temporary, exceptional problems. The logic behind the first and second criteria should be fairly clear. For the third reason, it is crucial that traffic management is not used as a means to avoid necessary investment in infrastructure. Due to the invasiveness of traffic management measures, as well as the risk for abusive re purposing of traffic management measures, the FCC should ensure that operators be as transparent as possible, in order to ensure that open internet provisions can be implemented effectively.

Conclusion 4: Traffic management is perfectly permissible, on condition that it is implemented in ways that are appropriate from a privacy, competition and economic

perspective.

Democratic and privacy concerns

A non-neutral network is one where the current open "any-to-any" nature of online communication is replaced with an entirely unpredictable any-to-"whoever the access provider allows you to access" system. Restrictions can be imposed on the basis of either economical concerns or on the basis of whatever other restrictions the access provider wishes to impose. We see this in the United Kingdom, where a voluntary "code of conduct" for net neutrality has proven entirely useless as a means to prevent arbitrary restrictions on access to content.

Taking the entirely legal and uncontroversial "order-order.com" and "jezebel.com" websites as an example. They were blocked by the ISP TalkTalk, meaning that they had no way of being accessed by over four million people in the United Kingdom. Going back to the question of competitive pressures, the injured parties (the two blogs) lost access to millions of possible readers while impact was exponentially smaller on TalkTalk's subscribers, only a small proportion of which will have been reading those specific blogs. In total, a test of the 100,000 top sites in the UK (as ranked by Alexa) found that almost one in five were blocked.[5] For this reason, it is crucial to ensure that any rules on blocking or other limitations be as broad as possible, in order to protect the free speech rights of individuals.

Conclusion 5: Rules that limit blocking should be as broad as possible and should not be restricted to anti-competitive behaviour.

Privacy rights are also under severe threat. The Body of European Regulators (BEREC) found that "when blocking/throttling is implemented on a network, this is typically done using deep packet inspection (DPI)". It is worth nothing that it is highly questionable as to

5 http://www.wired.co.uk/news/archive/2014-07/02/blocked-sites-filters

whether the use of DPI is lawful under European privacy legislation. Deep packet inspection technologies allow network operators to look "deeply" into packets of data passing through their networks and gain precise views of what data is being communicated from whom and to whom online.

It would be completely unacceptable if the FCC, as a US (independent) government agency were to act in a way that would facilitate such a restriction on the privacy rights of US citizens, which would, in turn, limit rights which are based on privacy, such as freedom of communication and freedom of association. The global impact on such as short-sighted position being taken by the United States would be hugely negative. Although his target was slightly different, the words of William E. Kennard in his post-FCC role in Brussels are apposite:

> *There is another specter lurking out there: that some governments will seize on the ETNO proposal for all the wrong reasons, because they want more control over the Internet for anti-democratic purposes. Why would you associate your businesses and your fine, iconic brands with an effort like that?*

Conclusion 6: Clear, comprehensive and well-enforced rules on net neutrality are needed. The alternative is a level of surveillance and restrictions which have no place in a democratic society.

Conclusion and recommendations

European Digital Rights firmly believes that reclassification under Title II will be the most effective and least bureaucratic solution.

This approach best fits with the unavoidable recognition that the internet is now a public space, on which we rely for our exercise of our democratic rights. Its economic and social

value is far too great to permit widespread experimentation by a small number of private companies.

The scale, motivations and range of types of discrimination that we can see in the US market and that we can anticipate based on the actions of access providers in Europe are such that overarching powers are needed by the FCC, beyond those that would be available under Section 706.

We also believe that attempting to find a solution under Section 706 will be more bureaucratic, more prescriptive and less future-proof than a reclassification.

Any outcome of this process which, in this weak competition environment can reasonably be expected to create a new "data reception" monopoly for access providers will be economically and socially damaging.

****