

## Comments on BEREC's Draft Guidelines for Quality of Service in the Scope of Net Neutrality

July 2012

### Preliminary Remarks

The Voice on the Net Coalition Europe ('VON') welcomes the opportunity to comment on the BEREC's public consultation on its draft Guidelines for quality of service in the scope of net neutrality (hereafter 'the QoS Guidelines').

Network operators' control over the physical last-mile infrastructure necessary to access the Internet allows them to effectively determine whether end users reach the Internet at all, and if they do so, what they can access. The problem is therefore centred on the Internet access bottleneck, and is particularly relevant in mobile markets, where only a limited number of providers exist.

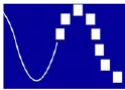
As shown in the findings from BEREC's and the European Commission's joint investigation, reflected in their 'View of Traffic Management and Other Practices Resulting in Restrictions to the Open Internet in Europe',<sup>1</sup> there is evidence in the market that many ISPs across the EU, especially when vertically integrated into the provision of content, services and applications, unduly manage traffic conveyed over their network. These practices include blocking applications and virtually foreclosing access to and use of content, applications and services provided by third party providers in order to secure (higher) revenues or other commercial benefits. So when looking at setting guidelines for QoS, BEREC should ultimately try to answer the following question: where does the line fall between 'legitimate' and 'harmful' network management, and hence QoS guidelines should focus on creating safeguards for the legitimate network management practices, all others being prohibited.

VON would finally like to urge BEREC to quickly create clarity in the area of net neutrality by ensuring, in collaboration with the European Commission, that guidelines are issued, and is supported in this view by the recent open letter by BEUC addressed to Vice-President Neelie Kroes<sup>2</sup>, in which they state:

---

<sup>1</sup> See BEREC. (2012). *A View of Traffic Management and Other Practices Resulting in Restrictions to the Open Internet in Europe – Findings From BEREC's and the European Commission's Joint Investigation* (BoR(12)30). Retrieved at, [http://erg.eu.int/doc/consult/bor\\_12\\_30\\_tm-i\\_snapshot.pdf](http://erg.eu.int/doc/consult/bor_12_30_tm-i_snapshot.pdf).

<sup>2</sup> See BEUC. (2012, July 16). *Protecting Net Neutrality in Europe. Letter Sent to the Vice-President of the European Commission Ms. Kroes*. Retrieved at, <http://docshare.beuc.org/docs/1/OHPHJKHDHDEMMPNMHPNEGMNIPDWY9DBKCY9DW3571KM/BEUC/docs/DLS/2012-00482-01-E.pdf>.



*“We thus call on you to undertake a new legislative measure which should include at least the following elements:*

- *A definition of the net neutrality principle.*
- *A definition of legitimate and illegitimate traffic management.*
- *A general prohibition of non-discrimination between Internet traffic streams unless done on legitimate traffic management grounds, and in particular a prohibition to violate the end-to-end principle.*
- *A clear set of obligations on ISPs regarding the neutrality and QoS of the Internet access services on the one hand, and on specialized services on the other.”*

### **Setting the Ground Rules First**

Though VON understands that the various aspects of net neutrality (differentiation practices and competition issues, IP interconnection and QoS) are quite complex, we believe that it would be important to frame the debate properly, and closely link these consultations and their recommendations together.

For example, when looking at the assessment of QoS in the two scenarios identified by BEREC (namely degradation of Internet access as a whole and issues regarding individual applications run over the IAS), BEREC should first identify which practices it considers admissible and which are prohibited, as well as the approach it proposes to take in this area. VON will briefly expand on both aspects below.

#### **1. Identifying Which Practices are Admissible and Which are Prohibited**

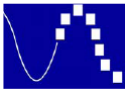
The burden for regulators and ISPs of QoS monitoring and setting of minimal requirements is to a large extent dependent on the room that is given to ISPs to differentiate in the traffic that goes over their network.

In her June 2012 White Paper on ‘Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like’<sup>3</sup>, Barbara van Schewick points out that working solely on a case by case basis without setting general guidelines beforehand is not the best approach:

*“Narrow decisions that are deliberately tied to the facts of the specific case and refuse to elaborate broader principles may not provide meaningful guidance for future cases. Thus, it is unclear whether and how quickly useful precedents will emerge. In the meantime, the costs associated with the uncertainty persist.*

---

<sup>3</sup> See van Schewick, B. (2012). *Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like*. p. 26-27. Retrieved at, <http://cyberlaw.stanford.edu/downloads/20120611-NetworkNeutrality.pdf>.



*Moreover, as set out in more detail below, the substantive principles emerging from case-by-case adjudications are less likely to adequately protect the values and actors that network neutrality rules are designed to protect. (...) Case-by-case approaches provide an advantage to well-financed actors and tilt the playing field against those – end users, low-cost application developers and start-ups – who do not have the resources necessary to engage in extended fights over the legality of specific discriminations in the future. Network providers and large application providers can conduct fact-intensive investigations, pay lawyers, economists and other experts to engage in the fight over the correct interpretation and the application of the rule at the regulatory agency and, later, in the courts, and employ lobbyists to organize support for their position in Congress or at the White House. End users, low-cost application developers and start-ups lack these resources. Thus, adjudications will likely be systematically biased against their interests. They are, however, some of the key groups that network neutrality rules are intended to protect.”*

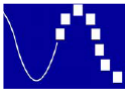
VON fully agrees with this analysis and urges BEREC to first and foremost draw the line between ‘legitimate’ and ‘harmful’ network management, and hence ensure that the QoS Guidelines focus on creating safeguards for the legitimate network management practices, all others being prohibited. This implies that in the steps identified in the QoS Guidelines on p. 31-32, a Step 0 should be added which covers ‘setting the ground rules for net neutrality protection in the EU’.

In other words, traffic management for the purposes of combating spam, security attacks or punctual exceptional measures to alleviate congestion are useful and should not be contested as such, as long as they remained proportional and not harmful.<sup>4</sup> Traffic management has always taken place in the Internet and VON considers there is no issue for ISPs to fairly use network management to overcome technical challenges and maintain a high quality Internet service for their customers. However, this freedom to manage the network should not be seen as an alternative to sustained network investment to meet large increases of capacity, which has characterised the Internet since day 1.<sup>5</sup>

---

<sup>4</sup> A point also made by BEREC in the QoS Guidelines, p. 6, both as regards congestion and network security and integrity management.

<sup>5</sup> The Canadian CRTC has very specifically stated in its Review of the Internet traffic management practices of Internet service providers: “36. The Commission notes that investment in network capacity is a fundamental tool for dealing with network congestion and should continue to be the primary solution that ISPs employ. However, the Commission considers that investment alone does not obviate the need for certain ITMPs, which may be used to address temporary network capacity constraints and changing network conditions, as well as for service innovation.”. See CRTC. (2009). Review of the Internet Traffic Management Practices of Internet Service Providers. Retrieved at, <http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm>



Moreover, it is important to keep in mind that academic research shows that the security rationale is “often used to justify practices that block traffic”, and therefore “this rationale should be divided into two categories — traffic management to address traffic potentially harmful to the user versus network management techniques employed by broadband Internet access providers to address traffic harmful to the network”.<sup>6</sup>

At the same time, this same research highlights that the congestion rationale is “often used to justify ISP traffic shaping on file-sharing traffic”, but “if the practice involves blocking without user choice’ this should then be classified ‘as unreasonable’”.<sup>7</sup>

Furthermore, traffic management should not be a license for ISPs to behave in anti-competitive and other harmful ways, such as blocking legitimate content and applications or unreasonably degrading services that users have paid to access. Such practices are often based on commercial motivations and are harmful both to end-users (both CAUs and CAPs)<sup>8</sup> and innovation generally. VON therefore considers that BEREC and its members should ensure that all end-users can continue to use the Internet applications, services and devices of their choice and access the content of their choice, as mandated by Article 8(4) g of the Framework Directive (FD) and that the principle of end-to-end connectivity set out under Art. 8(3) g FD is preserved.<sup>9</sup> BEREC and its members should therefore resist any attempts, whether regulatory, commercial or competitive, to block or hinder unfettered access to Voice over IP (VoIP) (or similar technologies) and more generally to all legal Internet content, applications and services, including their underlying technology, and that prevents VoIP from being utilised to its full potential.

VON believes that this objective is best achieved by clearly setting out principles for reasonable traffic management in line with the recommendations put forward by ARCEP, whereby traffic management practices should “comply with general principles of relevance, proportionality,

---

<sup>6</sup> See Jordan, S. (2010). A Framework for Classification of Traffic Management Practices as Reasonable or Unreasonable. *ACM Transactions on Internet Technology*, 10(3), 1-23. p. 15. Retrieved at, <http://www.escholarship.org/uc/item/3ng6r1fw>.

<sup>7</sup> See Jordan, S. (2010). *Ibid*, p. 15.

<sup>8</sup> For the sake of clarity, VON refers to the following concepts set forward in BEREC’s draft Report on ‘an assessment of IP-interconnection in the context of Net Neutrality’ (BoR(12)33): “Content and application providers (CAPs) create and aggregate content (e.g. webpages, blogs, movies/photos) [and] applications (e.g. search engines, messaging applications” (p. 11, including examples) and CAUs are “both, residential (private) users and business users of a broadband/Internet access in their function of passively consuming content” (p.12), read in conjunction with the clarifications provided on p.9, namely that “actual players will usually perform different combinations of functionalities (e.g. content and applications users may at the same time provide content and applications) along the value chain”.

<sup>9</sup> Though VON understands BEREC’s point on p. 10 that these articles should be read as setting goals, not as being tools in themselves, it is important that these goals be proactively pursued by BEREC and its members and that the QoS Guidelines ensure that all available tools are used to achieve these goals in the most effective and immediate manner. Leaving the current status quo certainly seems to contradict these policy objectives.



*efficiency, non-discrimination between parties and transparency*".<sup>10</sup> In her white paper, van Schewick for example develops the concept of 'user-controlled Quality of Service', whereby "network providers make different types of service available equally to all applications and classes of applications and where users choose whether and when to use which type of service".<sup>11</sup> She considers this approach to be the only one that responds to what she has identified as the three guiding principles required to safeguard net neutrality and the open Internet, namely: (1) application-blindness, (2) user choice and (3) innovation without permission.<sup>12</sup> As an illustration of such an approach, van Schewick states that: "For example, a network provider could offer a low-delay service, a best-efforts service, a less than-best-efforts service, and a guaranteed-bandwidth service. The decision of whether and when to use which service would be left to the user. For example, one user could use the low delay service for Internet telephony, another may use it for online gaming, and a third user may use it for e-mail, if that is what that user wants. This type of user-controlled Quality of Service is technically feasible".<sup>13</sup>

VON agrees with such a user-centric non-discriminatory approach and considers that BEREC should set in place the needed principles and safeguards to deliver such a result, which seems to equate to BEREC's definition of 'prioritised IAS' (p. 40) and its statement that "it may be relevant to prohibit application-specific restrictions on a general basis" (p. 59). Such principles could be seen as a form of minimum qualitative QoS, more detailed quantitative QoS being set separately.

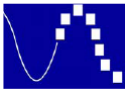
---

<sup>10</sup> See ARCEP. (2010, November 15). *ARCEP Has Published Ten Proposals and Recommendations for Promoting a Neutral and High Quality Internet*. Retrieved at, [http://www.arcep.fr/index.php?id=8571&L=1&tx\\_gsactualite\\_pi1\[uid\]=1317&tx\\_gsactualite\\_pi1\[annee\]=2010&tx\\_gsactualite\\_pi1\[theme\]=0&tx\\_gsactualite\\_pi1\[motscle\]=network%20neutrality&tx\\_gsactualite\\_pi1\[backID\]=2122&cHash=5575839c1d](http://www.arcep.fr/index.php?id=8571&L=1&tx_gsactualite_pi1[uid]=1317&tx_gsactualite_pi1[annee]=2010&tx_gsactualite_pi1[theme]=0&tx_gsactualite_pi1[motscle]=network%20neutrality&tx_gsactualite_pi1[backID]=2122&cHash=5575839c1d)

<sup>11</sup> See van Schewick, B. (2012). *Ibid.* p. xiii.

<sup>12</sup> More in detail, van Schewick (2012: xiii) points out that: "First, they preserve the application-blindness of the network: The provision of Quality of Service is not dependent on which applications users are using, but on the Quality-of-Service-related choices that users make; thus, the network providers does not need to know anything about which applications are using its network in order for this scheme to work. The network provider only makes different classes of service available, but does not have any role in deciding which application gets which Quality of Service; this choice is for users to make. As a result, network providers cannot use the provision of Quality of Service as a mechanism to distort competition among applications or classes of applications. Second, since users choose when and for which applications to use which type of service (in line with the principle of user choice), they can get exactly the Quality of Service that meets their preferences, even if these preferences differ across users or (for a single user) over time. Third, in line with the principle of innovation without permission, an innovator does not need support from the network provider in order for his application to get the Quality of Service it needs. The only actors who need to be convinced that the application needs Quality of Service are the innovator, who needs to communicate this to the user, and the user, who wants to use the application. This greatly increases the chance that an application can get the type of service it needs".

<sup>13</sup> See van Schewick, B. (2012). *Ibid.* p. 56. Van Schewick (2012: 58) does note that such an approach does not imply regulatory forbearance as "a network provider who is allowed to charge for Quality of Service has an incentive to degrade the quality of the baseline, best-effort service to motivate users to pay for an enhanced type of service. To mitigate this problem, the rules should require the regulatory agency in charge of enforcing the network neutrality rules to monitor the quality of the baseline service and set minimum quality standards, if the quality of the baseline service drops below appropriate levels".



## 2. Once the Framework is Set, What Will be BEREC's Approach (and the NRAs')

Article 22 paragraph 3 of the Revised Universal Service Directive stipulates that: *"In order to prevent the degradation of service and the hindering or slowing down of traffic over networks, Member States shall ensure that national regulatory authorities are able to set minimum quality of service requirements on an undertaking or undertakings providing public communications networks"*.

The use of 'prevent' does seem to suggest that any action undertaken by BEREC or NRAs should occur *ex ante* rather than *ex post*, as measuring what a network is capable of offering may be rendered more difficult once unreasonable traffic management practices have already been introduced. It is important to note again in this perspective, that blocking, degradation and other hindrances to services, applications and content that consumers want to access are already widespread as set out above. Where there is such evidence of harm, intervention would therefore be warranted, in the form of the imposition of minimum quality of service, whereby an end-user should always be able to access the best efforts, global public Internet, whichever other services they may also be subscribing to.

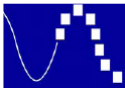
VON therefore considers that the only way to use the QoS tool provided by Art. 22(3) is by implementing a constant monitoring of all players on the market, both at a contractual and at a technical level, and to set upfront the QoS Guidelines at least at a qualitative level (*i.e.* what ISPs can and cannot do in terms of traffic management).<sup>14</sup> VON therefore recommends the adoption of broad guidelines highlighting principles supporting the protection of the open Internet, including what constitutes reasonable network management and minimum quality of service access to the Internet that could be enforced on a case-by-case basis.

VON would therefore propose the following changes to BEREC's statements in the QoS Guidelines: *"In order to identify cases of degradation of Internet access service (IAS) as a whole, it is necessary to monitor the service quality, ~~either proactively or~~ and reactively"*. (p. 5 – similar statements should be changed in the document, notably on p. 6). This is in line with BEREC's view that *"in order to detect a degradation of the general Internet electronic communications services, the performance must be monitored over time"* (p. 24).

From a practical point of view, we believe that the following elements are critical in determining and monitoring quality of service requirements from both a quantitative and qualitative point of view:

---

<sup>14</sup> A good starting point for such guidelines are the functional/qualitative requirements listed by BEREC in the QoS Guidelines on p. 23.



- The support of a body of technical experts, put in place through a multi-stakeholder approach that includes relevant industry segments (including CAPs), consumer organizations and civil society representatives;
- Regular testing of Internet speeds and quality of service for each access provider (fixed or mobile), both in terms of the speeds available for Internet access and for the various managed services, if any are available, and for each main application type such as streaming, VoIP, Peer-to-Peer (P2P), websites, etc. For managed services, SLAs offered could also prove a useful source of information; and,
- The requirement for ISPs to report on a regular basis to NRAs about the quality of services effectively achieved in the different layers of their network, both in the last mile and at hand-over points. Regular measurements by NRAs or another habilitated body will be required to verify if the announced performances by ISPs are met in practice. Most regulators could easily do this as part of their recurring reviews of broadband speeds.

We believe BEREC has all the pieces of the puzzle in its hands and just needs to put them together and give end-users in Europe the Internet they deserve.

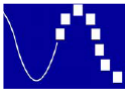
We refer you for more details to our answers below.

### Detailed Remarks

#### 1. What are your views on the criteria proposed for the assessment of degradation of Internet access service as a whole? (Ref. chapter 4)

VON agrees with BEREC's definition of specialized services as set out in the QoS Guidelines (p. 27). We also consider that a couple of remarks made by BEREC merit to be highlighted and receive more prominence in the final version:

- Degree of restrictions: *"According to the wording of this provision (Art. 22(3)) there is no requirement that the degradation, hindering or slowing down should be severe"* (p. 25). VON can only agree with this statement and encourage BEREC and its members to act upon it. VON also considers that 'severe' should be removed on p. 53, where BEREC seems to imply regulatory intervention occurs only after a *'situation of severe degradation'*, in clear contradiction with Art. 22(3) which requires preventive measures. BEREC also talks about the concept of *'adequate'* quality (p. 54), which could be open to interpretation.
- Link between specialized services and Internet access: though BEREC rightfully points out that each of these services run on different parts of the network, BEREC also rightfully states that



(1) “specialised services can provide a reference to which IAS can be compared” (p. 40), (2) “in cases where the performance of specialized services is actually increasing, the Internet access service should be assessed based on a similar increase in performance levels” (p. 24) and (3) “even though these are significantly different service categories, an assessment could be made as to whether specialized services are provided at the expense of Internet access services” (p. 41).

- Vote with your feet = vote with your wallet: “the price difference between the restricted and unrestricted offers must also be assessed as an element of the switching cost” (p. 53). From VON’s perspective, the fact that some ISPs ask CAUs for the payment for a surcharge to use VoIP apps on mobile phones is a clear abusive practice, notably when considering that: (1) the CAU and CAPs have both paid for their use of the network, as pointed out by BEREC in its IP-interconnection paper and (2) many of the VoIP apps are actually available for free or at a minimal charge.

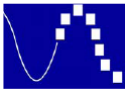
**2. What are your views on the criteria proposed for the assessment of issues regarding individual applications run over the Internet access service? (Ref. chapter 5)**

The joint snapshot of the market situation by BEREC and the European Commission has demonstrated that practices affecting individual applications or protocols such as VoIP and Peer-to-Peer are commonplace and hence more than “examples (...) that can be foreseen” (p. 35).

Indeed, as VoIP is particularly sensitive to degradations in network performance (especially in terms of latency requirements), and because of its reliance on P2P in some cases, it can be faced with various network management impediments put in place by access operators. Additionally, because the predominant VoIP protocols used today all generate P2P traffic (including SIP and H.323), they are at risk of being blocked or degraded as a result of blanket anti-P2P measures imposed by operators. It must hence be noted that P2P applications do not necessarily generate high bandwidth traffic as stated on p. 36. VoIP and video communications can be especially harmed by temporarily delaying sessions using peer-to-peer or other applications and protocols, due to their reliance on a steady stream of real-time communication packets.<sup>15</sup> Limiting or delaying a VoIP session or video communication can be tantamount to blocking, that is negating a user’s ability to communicate. Even when VoIP packets are delayed a mere 250 milliseconds, the lag is noticeable and impedes speech communications. Moreover, when looking at VoIP, hindering practices are not motivated by

<sup>15</sup> This is not to say that VoIP or video calling requires ‘guaranteed QoS’ – indeed, real time communications work well on the Internet when it is not subject to harmful traffic management. There is therefore no legitimate reason for that type of traffic to be harmfully and arbitrarily tampered with.





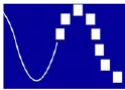
any need to manage congestion from a traffic management perspective, as VoIP traffic generally represents just a trickle of packets in today's growing broadband pipes. For most VoIP codecs, between 6 and 30 Kbps upstream and downstream is sufficient. In other words, VoIP services and applications do not consume substantial network resources (hence not justifying blocking or degradation on the basis of capacity constraints) and function today on fixed and mobile Internet around the world when left technically and contractually unrestricted.

In addition, as regards application-agnostic practices, VON would like to draw BEREC's attention to the risks that a 'like treatment' approach poses. Treating classes of applications differently for arbitrary reasons can have a harmful effect, notably if they can be seen to 'compete with other classes', particularly if these are provided directly by the network operator. As pointed out in van Schewick's white paper:

*"The positive stance towards forms of Quality of Service that provide like treatment is based on the assumption that discriminating among classes of applications that are not alike is socially harmless and should therefore be allowed. As this paper shows, this assumption is not correct. In many cases, discrimination among classes of applications hurts some classes of applications, even if the classes are not alike. For example, some Internet applications such as Internet telephony applications, Internet messaging applications or Internet video offerings compete with network-provider services that are sold separately from Internet access and do not run over the Internet-access portion of the network provider's access network. In these cases, discriminating against all applications in that class allows the network provider to favor its own offering without discriminating among applications within the class. Moreover, applications in a class can be harmed by differential treatment even if they do not compete directly with applications in other classes that are treated more favorably."<sup>16</sup>*

---

<sup>16</sup> See van Schewick, B. (2012). *Ibid.* p. xii. More specifically, van Schewick (2012: 50) describes the following situation : "For example, network providers usually like the idea of providing low-delay service to online gaming. Some online games are sensitive to delay, and charging the gamers for low-delay service would allow network providers to capture some of the value that online gamers realize from gaming. By contrast, network providers seem to be less interested in providing low delay service to Internet telephony applications like Skype or Vonage, since this would make these applications more competitive with the network providers' own telephony offerings. Thus, a network provider may decide to offer low-delay service only to online gaming, but not to Internet telephony, arguing that these are different classes of applications because 'gaming' and 'telephony' are different uses of the Internet. Internet telephony providers would argue that the correct class is 'applications that are sensitive to delay,' but their view would not matter until they had brought a complaint and succeeded in convincing the regulatory agency".



### 3. What are your views on the aspects proposed regarding the conditions and process for regulatory intervention? (Ref. chapter 6)

VON would first like to refer to its preliminary statements at the beginning of this paper, in which we set out the need for proactive intervention.

VON notes that both BEREC in this document and its other consultation documents, and the European Commission in various documents and statements, have pointed out the limitations that transparency and switching comprise in the context of net neutrality,<sup>17</sup> whilst recognizing that unreasonable traffic management practices do not only affect the users of the ISP adopting them, but also other users ('network effect', see notably on p. 35 and 44) and society in general (by affecting innovation and the socio-economic benefits it brings).

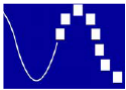
VON therefore considers that BEREC's answer to the question 'Is regulatory intervention necessary' on p. 43 lacks in nuances by seeming to imply that switching when there is a better IAS available is enough to allow NRAs not to intervene. Yet on p. 45, BEREC points out that sometimes there can simply be an 'unwillingness' to switch and details some of the factors at play. This concern is confirmed in the Eurobarometer Report, published by the European Commission on 28 June 2012, relating to customers' experience of Internet access and detailing QoS problems preventing them from using the content, applications, and services of their choice. The Report highlights that users report negative experiences, including of blocking and degradation, and provides a very worrisome assessment of customers' preparedness to switch to another ISP in response to negative experiences, notably given their concerns about the difficulties they expect to encounter in switching.<sup>18</sup>

VON considers that competition, transparency and ease of switching are just parts of the equation, seeing that even those markets which European regulators deem to be competitive (in particular the mobile retail markets) do not in fact exhibit the market dynamics leading to unrestricted access to the Internet. Transparent information tells consumers about the terms and conditions of their package, but does not offer them real choice nor unrestricted Internet access if operators mimic

---

<sup>17</sup> See European Commission. (2011). *Communication on the open internet and net neutrality in Europe*. p. 9 : "transparency and ease of switching are key elements for consumers when choosing or changing internet service provider **but they may not be adequate tools to deal with generalised restrictions of lawful services or applications**" [our emphasis added]. Retrieved at, [http://ec.europa.eu/information\\_society/policy/ecomm/doc/library/communications\\_reports/netneutrality/comm-19042011.pdf](http://ec.europa.eu/information_society/policy/ecomm/doc/library/communications_reports/netneutrality/comm-19042011.pdf).

<sup>18</sup> See European Commission. (2012). *Special Eurobarometer 381. E-Communications Household Survey*. pp. 26-28, pp. 31-32. Retrieved at, [http://ec.europa.eu/information\\_society/digital-agenda/scoreboard/docs/pillar/studies/eb\\_ecomm/summaries/eb381\\_summary\\_en.pdf](http://ec.europa.eu/information_society/digital-agenda/scoreboard/docs/pillar/studies/eb_ecomm/summaries/eb381_summary_en.pdf).

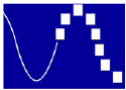


each other's behaviour – as experience in Europe demonstrates. Moreover, even if operators do not mimic each other's behaviour but CAUs are faced with a choice where there are only 3 operators on the market and operator 1 offers products A and B, operator 2 offers products A and C and operator C offers products B and C, that choice does not reflect the demand of the CAU that would like to benefit from A, B and C.

In her recent paper on 'Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like', Barbara van Schewick gives a very accurate description in this regards of behaviour displayed in the market by CAUs:

*"Participants in the network neutrality debate often assume that the viability of disclosure rules as a substitute for substantive regulation solely depends on the amount of competition in the market for Internet access services. After all, if there is no competition, there will be no other providers that consumers can switch to in response to discriminatory conduct, making it impossible for them to discipline providers. Based on this reasoning, participants in the debate often assume that mandatory disclosure alone will be sufficient to discipline wireline providers in Europe or in countries like Canada, where the market for wireline Internet access is generally more competitive than in the US. Similar arguments are made for mobile Internet access, where users often have a choice between three or more competitors.*

*These arguments fail to recognize that the market for Internet services is characterized by a number of factors – incomplete customer information, product differentiation in the market for Internet access and for wireline and wireless bundles, and switching costs – that limit the effectiveness of competition and reduce consumers' willingness to switch. Rules that require network providers to disclose whether and how they interfere with applications and content on their networks reduce the problem of incomplete customer information, though only to some extent. They do not remove any of the other problems. As a result, they still leave network providers with a substantial degree of market power over their customers that enables them to restrict some applications and content on their network without losing too many Internet service customers. Disclosure rules also do not affect the cognitive biases, cognitive limitations and externality problems that lead users to underestimate the benefits of switching providers compared to what would be in the public interest. Thus, even if there is competition in the market for Internet*



*access services, disclosure cannot replace substantive regulation as a tool to discipline providers.”<sup>19</sup>*

BEREC also states on p. 57 that: *“the first criterion when evaluating whether to impose minimum QoS requirement is the number of affected end-users”*. As BEREC has recognized that under Art. 2 FD, end-users comprise both CAUs and CAPs, so will the NRA need, for example, to think of all the employees of the hindered or blocked CAP affected by an ISPs’ practice? And all the potential employees that will not exist as innovation gets slowed down by allowing gatekeeping practices?

VON is also surprised by the level of detail BEREC goes into to describe the notification procedure, yet no mention is made about the necessity to set in place appropriate, efficient and speedy complaints procedures that are available to all end-users (CAUs and CAPs), even if VON is acutely aware of the limitations in terms of case-by-case approaches.

From a practical point of view, it is crucial for BEREC and its members to put in place appropriate complaints procedures for all end-users that would feel wronged, triggering own-initiative investigations by the regulator, and own-initiative enforcement by the regulator.

Decisions should be reached within a reasonable timeframe — for example 90 days from when a complaint is filed — and without unnecessary burden on the parties, including end-users and consumers. Reasonably speedy evidence gathering and decision-making will provide clarity to industry at the same time that it protects end users including consumers from ongoing abuses. Lengthy delays, in contrast, could prove harmful to the development of the Internet ecosystem by delaying the development and market entry of nascent services and thus depriving end-users including consumers of innovative new services and applications.

The experience of the Canadian Radio-television and Telecommunications Commission (‘CRTC’) may be instructive. In its October 2009 framework for evaluating the lawfulness of network management practices, the CRTC established a process whereby a party that believes that a network management practice is unlawful may file a complaint *“establishing that a (network management practice) discriminates or results in a preference or disadvantage”* and describing the rationale and evidence for concluding that the preference or disadvantage is unlawful.<sup>20</sup> The burden then shifts to the Access Provider to establish that *“any such discrimination, preference or disadvantage meets the*

---

<sup>19</sup> See van Schewick, B. (2012). *Ibid.* p. iv. Retrieved at: <http://cyberlaw.stanford.edu/downloads/20120611-NetworkNeutrality.pdf>.

<sup>20</sup> See CRTC. (2009). *Review of the Internet Traffic Management Practices of Internet Service Providers*. Retrieved at, <http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm>, and CRTC. (2010). *Modifications to Forbearance Framework for Mobile Wireless Data Services*. Retrieved at, <http://www.crtc.gc.ca/eng/archive/2010/2010-445.htm>.



requirement of the framework”.<sup>21</sup> CRTC also provided a mechanism by which Access Providers could obtain prior approval for a given practice, and it reserved the right to initiate an enforcement investigation on its own motion. VON encourages BEREC to study the CRTC approach, which has also the merit of having been tested – successfully – in practice already.<sup>22</sup>

VON finally considers that having independent measurement platforms in place and sharing of the collected data for research purposes and awareness raising must be ensured.

**4. To what extent are the scenarios described in these guidelines relevant with respect to your concerns/experience? Are there additional scenarios that you would suggest to be considered?**

As pointed out in our response to Q2, the joint snapshot of the market situation by BEREC and the European Commission has demonstrated that practices affecting individual applications or protocols such as VoIP and Peer-to-Peer are commonplace and hence more than “*examples (...) that can be foreseen*” (p.35).

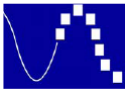
Indeed, the reported cases and public statements in the US and Europe -- *i.e.* the Madison River and Comcast cases in the US; Shaw Cable VoIP QoS fee dispute with Vonage in Canada; blocking or surcharging of VoIP and P2P notably by European MNOs in their terms and conditions; removal by some UK mobile operators of VoIP functionality from Nokia N95 handsets in 2007; statements by various telecoms CEOs in the press etc. – show that the threat is not hypothetical. In terms of the impact on innovation, the question should be asked which innovative content, application or service provider would be able to raise funds from investors for a new idea if there is no guarantee that this idea will ever be available to all end-users wishing to access it? Internet innovation was built around the principle that you could ‘innovate without having to ask permission’ and this principle which has underpinned twenty years of global, wide-ranging productivity growth and social progress would disappear in a context where broadband Internet access providers would be allowed to turn into gatekeepers.

\*\*\*

We thank you in advance for taking consideration of these views. Feel free to contact Herman Rucic, VON Europe, by phone (+32 (0)478 966701) or email (hrucic@voneurope.eu) should you need further information.

<sup>21</sup> See CRTC. (2010). *Ibid.*

<sup>22</sup> See CRTC Investigation Prompts Rogers to Stop Slowing Down Internet Traffic. *Digital Journal*. Retrieved at, <http://www.digitaljournal.com/pr/774757>.



\*

\* \*

### **About the VON Coalition Europe**

The Voice on the Net (VON) Coalition Europe was launched in December 2007 by leading Internet communications and technology companies, on the cutting edge to create an authoritative voice for the Internet-enabled communications industry. Its current members are iBasis, Google, Microsoft, Skype, Viber, Vonage, Voxbone and WeePee.

The VON Coalition Europe notably focuses on educating and informing policymakers in the European Union and abroad in order to promote responsible government policies that enable innovation and the many benefits that Internet voice innovations can deliver.