BEREC draft Report on the Net Neutrality Regulatory Assessment Methodology (17) 112

KPN response

KPN
PO Box 30 000
2500 GA The Hague
The Netherlands
Contact person: Paul Knol (paul.knol@kpn.com)

Reference: GCO/17/U/035

5 July 2017

1. Introduction

KPN welcomes the opportunity to provide input to BEREC's consultation on the *Net Neutrality Regulatory Assessment Methodology (17) 112* (1 June, 2017). The subject of this report is of great practical importance for the market and input of market parties is therefore equally important. KPN is member of ETNO as well as GSMA, that will present a joint response in this consultation. We support that response.

As the BEREC report rightly shows, the issues of measuring internet access quality – and even more traffic management practices – has many complex aspects. In order to improve consumer trust in results of such measurements it is very important that commonly shared views and methodologies will be developed in the market. Incomparable use of such methodologies results in adding to confusion rather than creating trust and transparency. We therefore think it is extremely important that BEREC takes the lead in communicating best practices, ensures prevention of wrongful application of tools and supports balanced communication. However, as we read the report, on some issues it seems worthwhile to consider standardisation rather than describing best practices. We believe that it is appropriate if BEREC would seek ETSI support – which involves all relevant market parties – rather than trying to define technical issues by itself.

In the Netherlands the issue of measuring internet access service quality has not led to earlier legislation (prior to 30 April, 2016), nor to defined measurement methodologies so far. However, prior to Regulation 2015/2120, internet access service providers already agreed to self-regulation in 2012 – under coordination of the Minister of Economic Affairs – on transparency measures for customers. In the absence of a defined monitoring mechanism this self-regulation merely contained obligations to inform customers on qualitative aspects of the quality of internet access services, on potential effects of the local customer equipment on the quality of internet access and how customers could influence the speeds they experience. The main parties to this self-regulation will send a joint response in this consultation, which we also support.

In addition to the above mentioned responses we like to strengthen some aspects that are of specific importance to us in the paragraphs hereunder.

Index

2. The regulatory requirements for assessment methodologies

The report covers 'regulatory assessment methodologies' for Art. 3 as well as Art. 4 of Regulation 2015/2120. It is important to note upfront the difference in these articles in relation to measurement methodologies.

Art. 4 relates to the quality of internet access services and mandate ISP's to include certain applicable information in contracts. The information to be included creates contractual rights and if an ISP does not comply to the contracted QoS contractual remedies by customers may be triggered. Art. 4 Par. 4 specifies that these remedies may be triggered if non-compliance of the contracted QoS is *'established by a monitoring mechanism certified by the national regulatory authority.'* It is obvious that the Regulation thus requires National Regulatory Authorities ('NRA's') to set criteria for monitoring mechanisms that can be certified. It is important that such requirements are technology neutral, objective, transparent, proportionate and – as far as reasonably possible – harmonised within the EU to avoid national fragmentation of technical requirements. KPN therefore supports BERECs intention to give guidance to NRAs on the relevant parameters and other aspects of such measurement tools.

Art. 3 on the other hand does not require NRA's technically monitoring traffic management of ISP's. It is highly questionable if such monitoring would be proportionate and necessary to verify compliance with the obligations of this article. Many circumstances influence the actual behaviour of (traffic over) networks, applications and services on the internet, as BEREC recognises. Measuring live traffic in order to control compliance will therefore be highly complex, will not lead to clear conclusions on the underlying reasons for differences (if any) in measurement results and may trigger questions in relations to GDPR as well as ePD/ePR obligations in relation to sensitive traffic data that would need to be analysed.[1]

We believe that such measurement results will furthermore most likely not demonstrate violations of Art. 3, but may lead to the need for operators to clarify all and every detail of findings, also of many influencing factors outside their control. Market reality shows that 'the internet community' is well aware of the obligations of Art. 3. In the reality of the market (perceived) violations are reported immediately. Even public websites such as *https://respectmynet.eu/* are available on EU level, where all potential violations of the net neutrality provisions can be notified without any threshold. BEREC fails to argue why compliance control based on complaints and market information would not be sufficient and ignores that such a way of working would be much more cost effective and proportionate than permanent measurement tools.

3. Measuring Internet access service quality

In our experience it is necessary to separate the two types of goals that BEREC mentions (QoS of IAS and measurement of traffic management) even further than is done in the draft report. On the top of page 5 BEREC lists the purposes for measuring IAS quality, but thereby includes e.g. 'detection of prioritisation' (third indent). However, the tools available to measure IAS quality are not suitable to include such type of detection and it is unlikely that these could be amended easily to such an end. Some of the other purposes (development over time and creating interactive maps) are also a different purpose than the compliance with Art. 4 of the Regulation and preferably should be separated.

As mentioned under point 1 above, Art. 4 Par. 4 requires NRA to certify mechanisms whereby contractual rights can be triggered. It is of utmost importance that mechanisms for this purpose are extremely reliable and predictable, because ISP's should be able to accurately contract on the QoS that can be measured with these tools.

[1] In its July 2013 reports on 'the analysis of data over and from' the four Dutch mobile operators the Netherlands Privacy Authority defined strict rules on the application of any data inspection technologies. The strict interpretation of the NPA most likely would also apply under future EU privacy regulation and also to the NRA's. It should be excluded that NRA's would be allowed to apply methodologies that ISP's themselves would not be able to use.

If these tools should also serve other purposes, NRA's should be extremely careful to judge upfront whether such a tool is or can be reliable for such other purposes. When the NRA itself – or third parties under some form of (implicit) approval of the NRA – would use results from the tool to inform the market on quality aspects of internet access services, the maximum certainty should be included that such information is comparable, technology neutral and up-to-date. Otherwise NRA's would unintendedly interfere in marketing of various ISP's services or (dis)qualifying some services over others without sufficient objective facts.

> It is important to note that IAS's are offered in strong competition (certainly in the Netherlands) and that ISP's are constantly investing in quality improvements in order to attract customers. As a result historic measurement data risk being outdated soon, especially if applied to specific locations and/or services. Publishing of outdated information could commercially harm ISP's, especially those that invest fastest. NRA's should therefore be utmost careful in using measured data for market communication. In our opinion the NRA should not have a role to provide 'customer information' in such a market, because the chances of informing incomplete or misleading data is far too great.

Currently available tools are mostly aimed at measuring the parameters of Art. 4 and not of 'individual applications using IAS'. We strongly question whether it would be useful to mix the measurements required under Art. 4 Par. 4 with other measurements.

BEREC recommends that a measurement server should be located 'at the national Internet exchange point (IXP)' (p. 5). That creates dependencies. ISP's can only control their own part of the total ('best effort') internet access service. If testing is done outside of their networks – implicitly – also other services (of third parties) would be tested. This would only work if full capacity and quality of these other components and services could be guaranteed. In practice this is hard to control. The risk is that not the service of the ISP is the limiting factor, but the capacity of links and servers outside the control of an ISP. This however should never be the basis to trigger contractual right for non-performance under Art. 4 Par. 4.

As acknowledged by BEREC, crowdsourcing based on in-browser or app-based monitoring tools include too many factors outside the scope of the ISP's IAS to be reliable for the testing of contractual rights as referred to in Art. 4 Par. 4 of the Regulation. Where and when NRA's should inform customers on available measurement tools it should be clear in communicating how results of such tools should be interpreted and that contractual rights cannot be based on such tools.

The BEREC report includes descriptions on how delay, delay variation and packet loss measurement should be done. We acknowledge that such data is useful for some customers and is relevant for the overall IAS quality, but to the majority of consumers it is complex to explain the relevance. In Art. 4 of the Regulation these quality aspects have rightly not been mentioned as a mandatory part of an IAS contract.[2] Therefore, when a tool includes such measurement possibilities, it should be made clear that the resulting data is not relevant for triggering contractual rights or grounds for termination, unless the contract has explicitly defined certain levels of quality in this respect. As for the accurateness of measuring these factors we refer to the ETNO/GSMA response.

Finally, the recommendation on page 9, to use base-10 rather than base-2 conversion rates should be discussed more in-depth. Until recently BEREC – in its Roaming Guidelines – announced its preference for base-2 conversion (1 : 1024). An unclarified sentence in the recitals of the recent amendment of the Roaming Regulation (promoting the base-10 conversion) has caused much uncertainty, as it has not been properly discussed and deviates from existing market practices. It is most unhelpful to have such an implicit 'note' in the draft report as basis to recommended deviating calculations. Would BEREC prefer the market to change more broadly the basis for calculations it would be preferred to have a separate open discussion with all relevant interest-

[2] Which it might be in the future, if the Commission's proposal of a European Electronic Communications Code would be approved and implemented. In the draft for Art. 95 Par. 1, Subpar. (i) these factors will be added to the existing framework.

ed parties (potentially also ETSI) before coming to conclusions. Otherwise such statement would only add to confusion.

4. Detecting traffic management practices that impact individual applications

As stated under point 1 above, tools designed for measuring traffic management practices are very different from quality of service measurement tools. In addition to the statements included in the ETNO/GSMA response (introduction under Par. 3 and under Par. 4) we would like to comment on this issue based on actual experience (with incorrectly applied tools).

In the Netherlands net neutrality regulation already entered into force in January 1, 2013 and we have already experienced discussions on presumed (unjustified) blocking practices in our mobile network based on independent (separately developed) measurement tools. It is very important to note that a very detailed understanding of data networks is necessary to draw conclusions based on measurements outside the network. A case that we have experienced was a test run by a university by using a VOIP client simulation, which found and published that we blocked certain traffic on our mobile network. After discussion and investigation we found that the research wrongly presumed that traffic that would be sent to any individual mobile connection should be passed through the network unrestricted even if no client was active on a device. Since traffic to a mobile connection would include the use of data for the mobile subscriber (at cost for that subscriber) the implementation is such that only traffic 'accepted' by the customer (e.g. by installing and activating an app on the device) will actually reach the device of the customer. If such security protocols would not be implemented, anyone could send undesired data to customers at their cost. The research thereby had to be rectified (as the researcher had to acknowledge the logic and importance of such implementation), but nevertheless the damage to our brand was done. It is extremely important to exclude such factors which may portray an incorrect conclusion. Limitations of the measurement tools used should be published. Communicating results should be done with utmost carefulness.

Furthermore we have experienced that some protocols for applications – such as the SIP protocol – allows for variation in technical details of implementation. Some implementations could lead to technical problems with certain mobile network settings (especially when NAT is necessary in the network), that can be remedied in the settings of the application and not easily in the network (since changing network settings may cause problems for other SIP implementations that did not previously experienced problems). The increasing variety of applications and network settings may cause similar problems with other protocols. Rather than 'measuring' networks, such situations require open communications between network operators and application providers to reach practical solutions and avoid burdensome discussions on principles.

Especially if crowd sourced measurement tools would be accepted, a relevant consideration should be how to deal with firewalls/VPN/anti-virus software, etc... installed by end users. Such software can be interfering with the testing capabilities and only few end users would be able to adept settings such that testing results would be reliable.

Detecting practices that impact QoS of individual applications describes two choices for Web browsing a normalized ETSI reference page (e.g. ETSI mobile Kepler page) or a page of a real website, both transparent options, while for Video streaming the first approach is to simulate a data stream comparable to a normal video streaming session. Simulating a service – as was done in the example described in the previous paragraph – is not a good practice since it can create unwanted conclusions due to the limitations of simulating a complex transport-channel instead of using a real service. It would be preferential to ask ETSI to create a reference or launch a video streaming session on an existing public streaming platform. Again, a cautious and transparency approach seems to be the best way to deal with such cases.

5. End user dependent factors that may impact the measurement results

BEREC rightly describes many factors within the end user environment – and thereby outside the scope of the IAS provides by an ISP – that influence the actual perceived quality by end users. Our own findings in pilots indicate that the vast majority of complaints about perceived quality relates to such factors. We support the ETNO/GSMA response in relation to this issue. These factors should be disregarded in measurement systems and, where that is not fully possible, the results of such measurements should not be accepted as a basis for defining contractual rights.

On fixed copper networks in recent years technological developments have allowed constant increase of speeds and quality, but the use of such technological changes require modems to be able to fully use the new standards. Where an ISP delivers the modem it could be held responsible for upgrading or replacing modems, but where free modem choice is applied it should be made clear that it is the responsibility of the end user to upgrade, maintain or replace modems in order to be able to use the QoS provided by the ISP.

6. Measurement results assessment

BEREC implicitly acknowledges that crowdsourced measurement approaches can easily result in insufficiently reliable data. It is extremely complex to (reliably) exclude all factors related to end user environment or other factors not related to the service of the ISP itself from the results. Furthermore, it should be guaranteed that the used data are representative and are not biased in relation to e.g. types of users, contracted speeds, relevant areas, etc. Therefore, we consider it most unlikely that such approaches could serve as bases for tools certified in accordance with Art. 4 Par.4 of the Regulation.

The definitions of the 'minimum', 'maximum', 'normal' and 'advertised' speeds as used in Art. 4 of the Regulation still leads to potential confusion. If comparability of such speeds would be intended then far more detailed definitions should be set and imposed. That would however require an additional effort to avoid implicit preferences for certain technical implementations over others, etc.

Under the Regulation its seems sufficient that an ISP communicates these speeds in a way that best meets its offered services. Measurement of compliance should then be done in line with the contracted QoS. If an NRA should wish to decide on more standardised approaches it would need to define such approaches in full and open consultation with all relevant market parties and should allow reasonable and sufficient time to adept existing approaches.

'Market level aggregation' as described by BEREC requires careful upfront consideration, e.g. 'What is the purpose of the (publication of) aggregated data?' If it is the intention to e.g. produce overall periodic (anonymised) results, the main issue would be to apply consistency in presenting the produced results. If, however, publications in relation to individual ISP's are considered, it is extremely important to secure that the results are based on verified data, without bias to technology, customer type, etc. If the results would be used to judge on compliance with the Regulation, it should be ascertained that the results are based on criteria that are available upfront. Undoubtedly there are more aspects here to consider, which means that individual NRA's must consult on such measures before introducing them in markets.

We agree with BEREC's conclusion that measuring individual applications is extremely complex and results cannot easily be drawn without further investigation, most likely asking an ISP for help to explain results of tests. Therefore it seems very questionable whether implementation of complex tools that would try to find 'questionable results' for certain (types of) applications would be proportionate and effective. Only if such tools would be used in a 'complaint-driven' manner, an excessive use of data-inspection techniques could be avoided.

7. Certified monitoring mechanism

BEREC indicates that the Regulation does not require Member States or NRA's to certify a monitoring mechanism. We agree to that conclusion, but on the other hand Art. 4 Par. 4 requires that facts to support a claim for non-performance of a contract should be based on a certified monitoring mechanism. That would imply that without such certified mechanism no such claim can be made.

In general we can support the considerations BEREC lists under Par. 7.1 of the report for an NRA to define certified monitoring mechanisms. Accuracy of the results should be guaranteed.

If certification is done on national level it should be ascertained that the criteria are transparent, reflect accuracy of measurement of the ISP service, and can be applied by end users. Some NRA's have undertaken to develop specific tools for this purpose, others have not done so (yet). As stated already in the introduction we strongly believe that customer trust and 'fairness' of publication of results would be greatly helped by more advanced and standardised approaches. Debates between customers, ISP's and NRA's can only be balanced if the criteria to be applied are proportionate and effective to give relevant information on the service offered by the ISP. By striving to improve such methodologies international standardisation (in ETSI) might not be the shortest, but ultimately the most realistic, way forward. Thus, upfront clarity on what is measured and how the results should be interpreted are best served.