14 March 2017

Written response to questions for BEREC stakeholder meeting with representatives of end-users and CAPs on 14 March 2017

Co-drafted by

Supported and edited by the EDRi Brussels Office.

Introduction

European Digital Rights (EDRi) is an association of civil and human rights organisations from across Europe. We defend rights and freedoms in the digital environment.

We welcome the invitation by the Body of European Regulators of Electronic Communications (BEREC) to represent the views of civil society in this Stakeholder meeting. This document is our response to the questionnaire we were provided in preparation of this meeting. We want to thank BEREC for the continued discussion with relevant stakeholders on the questions surrounding the implementation of the net neutrality provisions in the Telecom Single Market Regulation 2015/2120 (the Regulation) and the BEREC guidelines (BoR (16) 127) (the Guidelines).

Topic 1 – Measurement methodology / individual applications

A Network management set-up has to meet the following criteria in order to allow for confidence in the quality of the data collected and the reproducibility/comparability of the conclusions drawn from that data:

1. **Open Methodology –** the specification of the technical measurement and analytical choices about processing and aggregating the data have to be published in full detail and be up for consultation and peer review. The measurement methodology greatly influences the strengths and limitations of the test results. Stakeholders basing their decisions on the measurement data have to be informed about the underlying assumptions. For the completion of the digital single market, this methodology should be established by BEREC to allow for comparability across countries and between the various operations by multinational ISPs. Finally, the methodology should be oriented towards real quality of experience of the user and not theoretical maximums of the network and it should be built on the principles of privacy-by-design to avoid collecting measurement data that can identify individual users.

2. **Open Data** – measurement results should be accessible in an open, machine readable form under a free licence via a centralised platform[1]. This is the only option that allows for independent research and interpretation of the data by experts which can identify potential net neutrality violations based on large data sets. The central platform should allow access to the same, standardised data from all countries to allow meaningful cross-border evaluations.

3. **Open Source** – the measurement tools which are developed, used or propagated by NRAs should be open source and, if at all possible, published under a free software

[1] See the principle of the open definition for further guidance: http://opendefinition.org/od/2.1/en/

licence. Only by independent evaluation of the code base and technical specifications of the actual measurement tools, the measurement server instrumentation and hardware and an indication of the infrastructure paths can it be ensured that the measurement is functioning as set out in the published methodology. Publishing the source code enables trust in the functioning of the software and allows the community to audit the software for bugs and systematic errors in the measurement process. In situations where the software requires installation on the terminal equipment of the end-user, it is a reasonable expectation for someone in the technical community to be able to review the source code for potential vulnerabilities or unexpected behaviour before installing the software. Similarly, it can be argued that the Regulation guarantees the right to access the internet from a terminal equipment of the end-user choice. Hence, the measurement tools safeguarding this right have to be (at least in theory) available on all software platforms. Only free and open source software satisfies this requirement as it allows users to modify the software to run on their operating system.

In order to measure net neutrality violations, it is important to categorise the various forms of violations that a NRA should be seeking to identify. We therefore offer the following categorisation:

1. Active Discrimination

1.1 Blocking specific end-points, applications or classes of applications

Except for the specific cases in Article 3(3)(a) and (b) of the Regulation, there are no grounds for blocking end-points, applications or classes of applications. Examples of such practices would be where a provider woulddisallow users to run their own Web server or prohibit the use of VoIP or MoIP applications. Blocking for security reasons, under Article 3(3)(b), should be limited to what is strictly necessary and must be proportionate to avoid overblocking and undue restrictions to the freedom to conduct business, freedom to seek, receive and impart information. A widely used application should not be blocked because there is some malicious use (such as in the case of Talktalk[2]).

1.2 Unreasonable Traffic Management

1.2.1 Throttling of individual applications

Handling specific classes of traffic or specific applications differently on a deliberate basis. For example, throttling peer-to-peer network connections.

1.2.2 Prioritising of individual applications

Prioritising own applications (such as own video on demand or music streaming services) for commercial reasons. Also the prioritisation of speed tests is an endemic problem that needs attention in the context of the issue of measurements.

1.2.3 Discriminatory Congestion Management

[2] http://www.ispreview.co.uk/index.php/2017/03/uk-isp-talktalk-blocks-teamviewer-vpn-service-scammer-fears.html

Exceptional network management in cases of impending network congestion shall not differentiate among equivalent categories of traffic, in line with Article 3(3)(c).

1.2.4 Discriminatory treatment of traffic after the data volume has been exceeded

A particular distinction should be made in case of network management after the data volume of a contract has been exceeded. BEREC clarifies this potential violation in paragraph 55 of the Guidelines.

1.3 Zero Rating

Zero rating means not counting data of specific applications towards the end user's data volume.

2. Passive Discrimination

2.1 Allocation of bandwidth

Using a large fraction of the available (last-mile) bandwidth for the ISP's own applications (e.g. specialised services) and only a smaller portion for the open internet. The Regulation requires the provision of specialised services not to be detrimental to the quality and availability of internet access services (IAS). If a large fraction of the last-mile bandwidth is used on the ISP’s own services, the IAS will be almost indistinguishable from a sub-internet service, which is clearly prohibited by the Regulation and the Guidelines.

2.2 Offering sub-par bandwidth and/or lower data volumes than the technology would enable

- Artificially limiting the enduser's data volume or offering slower end-user (last mile) bandwidth connections than the current technology would enable.
- Artificially slowing down the progress and/or adoption of new technologies (e.g. 4G LTE) in the field of (mobile) networking technologies.
- Reserving a large fraction of the bandwidth for roaming customers from other Member States, which pay per megabyte traffic (via the wholesale market) while domestic customers have prepaid data volumes, should also be viewed as passive discrimination.

2.3 Discriminating between traffic through deliberate topology (interconnect/peering) choices

Artificially and deliberately limiting the connection (bandwidth, speed) to other autonomous networks, uplink/backbone Tier 1 providers, CDNs, or application servers. Demanding higher than technically justifiable interconnection/peering fees (double-sided market issue).

Question 1) How should regulators monitor the net neutrality obligations? For example, what would be the best way to detect traffic management practices that affect quality of service of individual applications used over an Internet access service?

NRAs should provide or contribute to the necessary infrastructure and software tools to enable themselves, a diverse group of users, and CAPs to run a variety of network measurements and thereby establish a common, openly accessible data set on the quality of individual applications, classes of applications, and the internet access services on a whole. Such global data sets enable NRAs and other interested stakeholders to evaluate the quality of applications in any given network and identify problems such as throttling, interconnection issues or a deterioration of the overall quality of internet access services.

This global approach has to be complemented with measurements that test a specific hypothesis of common net neutrality violations in a given network (e.g. blocking of VoIP, prioritising only some video-on-demand applications, throttling of file sharing, prioritising speed tests, etc.).

Question 2) How could regulators collect information from end-users and how should this information be used in the assessment? How could CAPs assist in detecting net neutrality violations?

We recommend using the platform www.RespectMyNet.eu – a joint initiative by civil rights groups including EDRi, IT-Pol, epicenter.Works, La Quadrature du Net, Bits of Freedom, Access Now, Digitale Gesellschaft, Nurpa, Open Rights Group, Xnet and several individual contributors. RespectMyNet allows users to submit information about potential net neutrality violations and attempts to further investigate the submissions received, filter out those which are not a violation within the current telecoms framework and submit the substantial cases with ample evidence to the responsible NRA. As civil society actors, the most significant difficulty we currently experience is the complete lack of funding to invest in the necessary research and development work that this platform requires. Such an undertaking should in principle be the responsibility of the NRA.

CAPs often conduct their own measurement operations to identify quality of service problems in a given network. NRAs should also offer those operators the possibility to run measurement servers within their network with a testing protocol which is similar to the application the CAP provides. A testing suite similar to the Network Diagnostic Test (NDT), Neubot or MeasurementKit provided by M-Lab, which measures network performance between a user and a specific measurement server, could then include this test case, which could be made indistinguishable from real user traffic.

Question 3) What are the main advantages and drawbacks of using KPIs (connectivity, time needed to load a web page, quality of a video streaming, etc.) to inform end-users about the quality of service and to detect of net neutrality infringements like blocking and throttling of applications?

The main use of KPIs is to inform users about the quality of their internet connection. The currently available information about the theoretical maximum of an internet connection does not allow for an informed comparison of internet access offers.

Although end-users have the right to certain information under the Regulation and ISPs are required to provide this information to users, according to paragraph 190 of the Guidelines, we have found that specific requests to ISPs about those and other KPIs are not answered, even for existing contracts.
Hence, the question about potential drawbacks of this information is not relevant as users were never even offered what the Regulation guarantees them. NRAs should monitor this closely and enforce the Regulation accordingly.

Question 4) What are the most important KPIs that should be measured? Should some of these KPIs be measured on a regular basis or on targeted situations? Any other advice on how to perform the measurements and the assessment of the measurement results?

The following Key Performance Indicators (KPIs) can best describe an internet connection:

1. Download speed
2. Upload speed
3. Packet Loss Rate
4. Latency
5. Jitter (variation in latency)
6. Quality of IP address (dynamic or static, shared or public, IPv4 or IPv6)[3]
7. Throughput

Because quality of service of many applications is sensitive to delays or loss of even single packets, care should be given to capture. In addition, various confidence intervals should be specified for each numerical indicator. Furthermore, these intervals should be large enough in order to account for the fact that even simple actions, such as loading a web page, can result in the transmission of thousands of network packets, where in the ideal case no degradation would occur in the transmission of any single packet.

In the context of net neutrality violations and compliance with the contractually agreed IAS quality, measurement methodology should be oriented towards the quality of experience of the end-user. This means the measurement should be oriented towards a real life full-path

[3] We want to stress that the full IP address is considered personal data and should not be collected as part of the measurement. Yet, the quality of the address and potentially parts of it can still be relevant in this context.

performance which crosses interconnection boundaries and should be done on a regular basis, including at peak-hours. Single-threaded tests should be preferred over multi-threaded tests in order to avoid obfuscation of deficiencies in the connection. In general, the measurement methodology should aim at capturing the real experience of users as closely as possible and not measure uncongested theoretical maximums within the network of the ISP at times when most people do not use the Internet. Otherwise, the NRAs would not fulfil the obligation set forth in the Regulation, i.e. to monitor traffic management practices, interconnection issues, or normally available internet speeds.

There are various factors that can influence those KPIs in any given situation:

1. Network Management practices which apply to the internet connection (types of reasonable network management, impending and actual congestion management)
2. Real-world (average) up- & download bandwidth and latency to specific applications and classes of applications (e.g. Web sites, e-mail, YouTube, Skype, Netflix, gaming, peer-to-peer traffic, etc.)
3. Bandwidth and latency to other users in different countries / continents
4. Limitations on data volume (how is it counted, really unlimited or fair use, what does fair use mean)
5. Number of concurrent connections
6. Location of the measurement in case of mobile networks[4]

Topic 2 – Measurement methodology / IAS as a whole

Question 1) What actions, knowledge and measurements could be requested from end-users to check whether the Internet access service performance meets what has been specified in their contract?

Measurement tools should be as easy to use as possible and not require any prior knowledge about the technical set-up of the internet connection. End-users should be treated equally. End-users do not always have advanced digital skills. Users without advanced digital skills also have a legitimate interest to measure their internet connection and to rely on the tools provided by his or her NRA. Moreover, end-users have a legitimate interest to measure the information about other variables (wifi or cable connection, contract or type of access technology, parallel applications with network activity) which can be vital for the assessment of the measurement data created. Therefore, we propose a two-step system:

First, the user should be given the possibility to run a simple one-click speed test which can measure overall and application-specific performances.

Secondly, the user should be asked a variety of optional questions which can enhance the measurement with metadata and thereby make it more specific and, therefore, more comparable. If end-user environmental factors such as his/her WiFi connection affect the

[4] For privacy reasons location information should be obfuscated to be less accurate

measurement, this is likely to show up in widely different measurements from different end-users, and the NRA can take this into account based on the information provided in the second step. The measurement should not automatically invalid or less accurate just because it was done over WiFi. On the contrary, it would be a more realistic end-user performance that is closer to the quality of experience of the user. Users should therefore be encouraged to run a measurement as often as possible, although the individual measurement cannot be taken as sufficient evidence to start official proceedings against an ISP. In this regard, NRAs should be encouraged to investigate *ex officio*.

A negative practice[5] would be a test which first asks the user a lengthy array of questions which discourages them from even starting the actual measurement process and thereby not gaining any information at all about their internet connection.

Question 2) Which minimum technical conditions (e.g. measurement metrics, measurement duration or number of samples) should be satisfied, from your point of view, in order to ensure that measurements correspond, with a sufficient accuracy, to the delivered Internet access service performance?

The accuracy of any measurement increases with the sample size. As the number of variables (environment specific factors) to account for is unknown, the exact number of measurements for any specific connection cannot be definitively determined. This is why a centralised, comparable open data set is a vital precondition for serious enforcement work. Only with such a system can statistical methods be used to identify structural problems in the network.

As specified above, we recommend a two-step system that collects optional data about each measurement from the user and then enriches the measurement with this complementary data. With more information, the individual measurement could be weighted with a higher accuracy in the overall picture created about the network.

If provided with a global and complete set of data, NRAs and independent researchers will be able to evaluate the quality of IAS in a given network, potential quality deterioration of the quality of IAS over time and differences between the contractually agreed and the actually delivered speeds.

Question 3) Which end-user environment specific factors (e.g. WiFi and cross-traffic) should be taken into account when assessing the validity of measurement results? How could these factors be detected and assessed in crowd-sourcing and software-based measurement set-up?

The following factors can have an impact on the results:

[5] https://breitbandmessung.de/

1. End-users device and software (device or software can slow down the performance of the connection; some browsers can become overloaded when too many tabs are active)
2. Quality of the local network (WiFi has inherent speed and QoS limitations)
3. Chosen data plan (maximum bandwidth, as defined by the service contract(s))
4. Network congestion or inter-connection effects
5. Server-side (application) effects (what is the maximum bandwidth the server of the specific application can deliver, load balancing issues, etc.)

Factors 1-3 can be accounted for by the user depending on their technical skills and expertise. Factors 4-5 are mostly out of the control of the average user – with some exceptions. For instance, congestion can usually be detected by increased packet loss. In light of these circumstances, measurements are always influenced by a multiple factors. Yet, all of these factors can be accounted for by a large sample and potential complementary information provided by the user. The expectation from user-driven measurements might not always be that they provide sufficient evidence to start official proceedings against an ISP, but they can and should be taken as a starting point for an investigation in potential non-compliance with legal obligations and further gathering of evidence.

Topic 3 – Practical considerations regarding implementation of QoS measurement systems

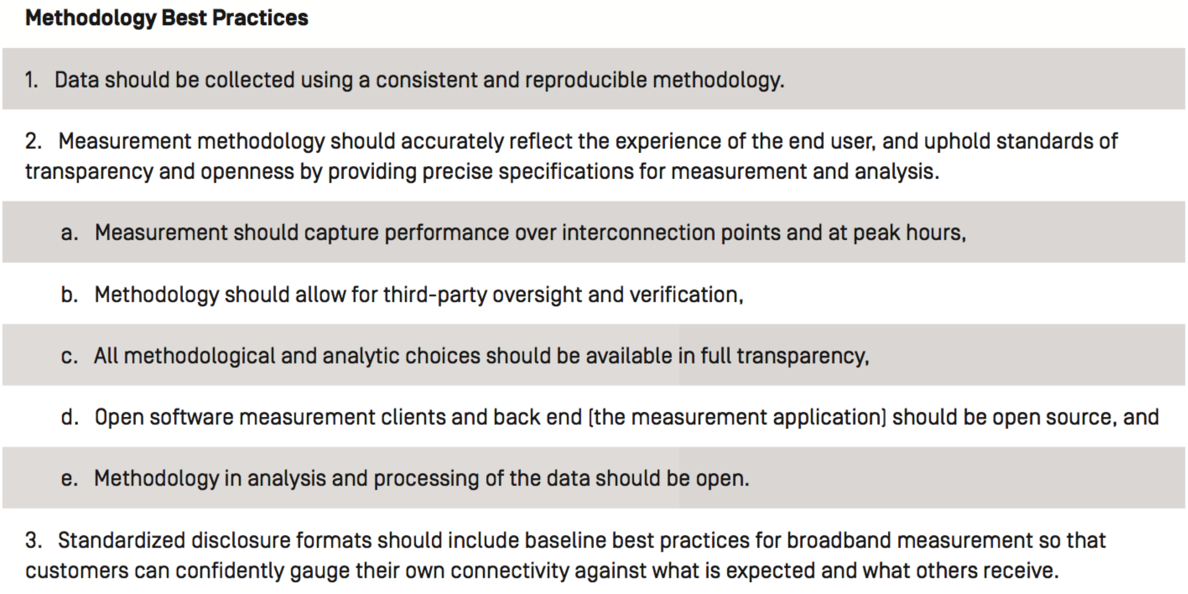
Question 1) Governance aspects What are your views regarding aspects such as:
How can regulators increase stakeholders' trust in regulatory QoS measurements?
How can BEREC play a role in that regard?
How should governance of QoS measurement systems and running of QoS measurement campaigns be handled by regulators?
Which role should open source software play in this regard? How should a system with collaborative administrations be managed?

We reiterate our three initial points about the measurement operations of NRAs which we see as indispensable preconditions for the success, trust and acceptance of the operation:

- Open Methodology – the measurement methodology has to be completely open, and peer-reviewed. The methodology has to be oriented towards the real life user experience and comply with EU rules on privacy and data protection.
- Open Data – the collected measurement data has to be accessible under the principles of open data in a centralised platform. The data has to be standardised to allow an easy comparison and analysis across countries.
- Open Source – The full set-up of the measurement infrastructure and the software used and the particular infrastructure decisions have to be made public and if at all possible freely licensed.

We propose that BEREC and NRAs cooperate with existing measurement projects like Measurement Lab to help the regulatory community build on existing best practices, software tools, testing infrastructure and open data platforms.

In this context, we also want to reference the "Key Recommendations for Measuring Broadband Performance" in the New America's Open Technology Institute study "Getting up to speed: Best Practices for Measuring Broadband Performance" from June 2016[6]:



Methodology Best Practices

1. Data should be collected using a consistent and reproducible methodology.

2. Measurement methodology should accurately reflect the experience of the end user, and uphold standards of transparency and openness by providing precise specifications for measurement and analysis.

   a. Measurement should capture performance over interconnection points and at peak hours,

   b. Methodology should allow for third-party oversight and verification,

   c. All methodological and analytic choices should be available in full transparency,

   d. Open software measurement clients and back end (the measurement application) should be open source, and

   e. Methodology in analysis and processing of the data should be open.

3. Standardized disclosure formats should include baseline best practices for broadband measurement so that customers can confidently gauge their own connectivity against what is expected and what others receive.

Question 2) <u>Security, reliability, availability etc.</u> What are your views regarding aspects such as:
- Which security measures should be taken to ensure confidentiality, integrity and availability of measurement results and measurement systems?
- How should collection and post-processing of measurement results be conducted?
- How should crowdsourcing be organized to increase representativeness of measurement results?
- How should publication of measurement results be handled by regulators? Which precautions should be taken if results are provided as open data?

The measurements provided by end-users should be anonymised immediately directly on the measurement system itself or immediately after the NRA or the collecting system has received them. This is important for maintaining end-user trust and for encouraging as many end users-as possible to submit measurements and use the tools provided. When measurements are provided by end-users, some measurements will unavoidably be inaccurate for a number of different reasons, e.g. the end-user environment. The best way to deal with this problem is by having independent measurements from many end-users as possible so that aggregate numbers do not reflect these inaccuracies. This requires end-user trust in the reporting system.

[6] https://na-production.s3.amazonaws.com/documents/MeasuringBroadband.pdf

We do not see a noteworthy risk of fraud in end-user reporting. The borderline cases can be handled with simple means, such as limiting the number of measurements that can be submitted from a given IP address (taking into account end-users with CG-NAT connections). Requiring end-user identification through eID or similar to combat a very theoretical risk of fraud in reporting potential net neutrality violations will be severely detrimental to encouraging end-user participation in the reporting mechanism and ensuring end-user trust that the measurements are handled anonymously. This is irrespective of whether the measurements are made available to others as open data or just used by the NRA.

We stress that the measurements should be made available as open data, and that data protection practices in place should b such as to ensure that the collected measurements can be made available to others as open data.

Question 3) System architecture aspects What are your views regarding aspects such as:
- What kind of measurement clients should be used (downloadable software and/or dedicated hardware probes, random subscriber lines and/or dedicated test lines, end-user-initiated and/or automatic application-associated, etc.)?
- What kind of measurement servers should be used (characteristics of the server, characteristics of the network connectivity of the server, location and distribution of the measurement servers)?

Measurement servers should run open source software, since this provides the best foundation for independent verification of the conclusions drawn from the measurements as well as overall transparency. The location of the measurement servers should correspond to the traffic patterns and traffic destinations of end-users. In particular, the location of measurement servers should allow for testing and investigation of possible net neutrality violations that may occur in interconnection agreements.

The tests should measure the overall performance of the IAS, but also the performance of individual, real life applications. For the second purpose the regulators should build upon existing open-source testing software (e.g. the aforementioned Network Diagnostic Test) and in general contribute to an open source software suite. In general, the system should be built with a modular design approach that allows for new protocols, measurement servers and testing cases.

Dedicated hardware platforms for testing purposes like "Measuring Broadband America" have proven problematic in this context as they did not satisfy the transparency requirements necessary to inspire trust in the results of the measurements[7].

[7] See page 14-16 in the New America's Open Technology Institute study "Getting up to speed: Best Practices for Measuring Broadband Performance" from June 2016.

Topic 4 – Net neutrality supervision tools and methods

Question 1) Network diagnostic tests: Could you point us towards existing (or concept of) tools and methods that allow end users or regulators to identify and assess traffic management practices, such as:

- **Prioritisation (of some users, of some protocol, content, or application)**
- **Blocking or throttling (of some users, of some specific content or application types (e.g. VoIP, streaming, peer-to-peer file sharing, newsgroups)) or some port or protocol (e.g. SMTP), or prohibiting some practices (e.g. use of VPN, tethering);**
- **Modifying the data transmitted e.g. via Image or video compression, or stripping out advertising;**
- **Use of DPI**
- **Provision of specialised services (if different from the above)**

We recommend using the tools included in RespectMyNet.eu[8]. Most of these tools require more development work so they are updated to the applications which are currently widely used. As NRAs have funded the development of testing software in the past, it would be advisable to build upon existing open source projects. Diagnostics tests that mimic peer-to-peer traffic, either bulk or interactive, are probably well-suited to detect net neutrality violations. This could also be an area of cooperation with CAPs (one-click hosters, VoIP, email or VoD providers), as they might often be very interested to have their protocols tested on a wide scale basis to identify potentially fraudulent traffic management in particular networks.

Regarding commercial practices and technical measures which are not in line with the Regulation, we advise NRAs to regularly screen the advertisements, terms-of-service, order forms, default configuration of customer premise equipment and other contexts where ISPs are very often quite blunt about the net neutrality violations which they intend to impose or already impose on their users. Some EDRi members use these sources on a regular basis to gather evidence that we then bring forward to NRAs. Similarly, these public offers are also a good starting point for investigations regarding existing or planned specialised services.

Regarding the use of DPI, the (planned) roll-out of products which are based on application-specific payment options are a clear indication of potentially illegal traffic management equipment, which is in breach of the Regulation, and commercial practices which are subject to a case-by-case evaluation, in line with BEREC's Guidelines on net neutrality.

[8] https://respectmynet.eu/start/

Furthermore, EDRi encourages NRAs to run exploratory measurements to test for common types of net neutrality violations. For example, the manipulation of transmitted data can be easily detected. . Similar tests offer evidence about the prioritisation of certain applications, but not others.

It is unavoidable that there will be disagreement about the interpretation of network diagnostics tests and measurements of possible net neutrality violations. The best way to address this is to ensure that the software used for all measurements is fully transparent, ideally free software, and that the individual measurements are made available as open data for analysis by NRAs, NGOs and CAPs. This requires data protection by design with complete anonymisation of the individual measurements in order to secure end-user trust. Having a large number of measurements reported by end-users is the best way to deal with inaccuracies due to local factors (such as WiFi), and the open data approach allows for different opinions as to how the results should be interpreted.

Question 2) End-user reporting platforms: How would you best configure / implement end-user reporting platforms to ensure a crowdsourced supervision of technical and commercial practices falling under art. 3 of the Open internet Regulation?

With the experience of RespectMyNet.eu, we have realised the importance of promoting and using such a platform. Civil society is well suited to running such a platform with the required end-user trust and the capacity and role to inform the public. However, civil society needs the necessary funding to improve the tools at hand, to evaluate the many cases that are reported and to build a fully informed case on them that can be brought to the corresponding NRA.

Question 3) Regulatory questionnaire: How would you best organise regulatory data gathering campaigns to ISPs, in order to get as much and as precise as possible information on their technical and commercial practices falling under art. 3 of the Open internet Regulation?

It is especially important that NRAs ask ISPs to provide information on specialised services, since this information is not publicly available and generally cannot be discovered with diagnostic tests performed by end-users. NRAs should also ask ISPs about traffic management systems and routers that are configured to deviate from the best effort principle in order to optimise traffic. This information is, of course, proprietary, but NRAs need this information to compare the traffic management information provided by ISPs with diagnostics networks tests performed by end-users. Unexplainable differences are likely to indicate net neutrality violations or at least traffic management systems that the ISPs have not accounted for. Similarly, information regarding any planned acquisition or operation of DPI equipment should be regularly sought from all ISPs.

It would be very helpful for independent researches and civil society if the result of such questionnaires were to be published, at least in an anonymised form.

Question 4) Other tools and methods: Which additional tools could you suggest to NRAs? E.g. campaigns to review ISP's terms and conditions, partnerships with consumer / citizen associations, universities, content and application providers, or other players

All zero rating pricing schemes should be reviewed carefully by NRAs. Content bundles and strategic partnerships with CAPs should also be reviewed even if the traffic is not directly zero-rated since these contractual arrangements give ISPs a potential economic incentive to inplement discriminatory traffic practices.

Question 5) General recommendations: Would you have any general recommendations to NRAs how to best supervise the implementation of art. 3 of the Open internet regulation?

It would be good that Member States were to increase regulators' resources to properly abide by the monitoring and enforcement obligations set forth by the Regulation. It is also important that Member States devote efforts in making sure BEREC and NRAs are and remain transparent and impartial. NRAs should proactively seek to monitor and enforce the Regulation *ex officio*. In addition, EDRi encourages BEREC and NRAs to cooperate with end-users, NGOs and CAPs that have an interest in making sure there are no net neutrality violations. An open data approach where network diagnostics tests are reported anonymously by a large number of end-users is the best way to deal with possible sources of errors in individual measurements and different opinions about how the results should be interpreted. Finally, we reiterate the need to fund civil society groups, including EDRi members, that have the expertise regarding net neutrality, so they have sufficient resources to help NRAs in monitoring and enforcing the Regulation.

Annex: Stakeholders optional technical questions

Governance aspects

Question 1) How should a measurement system with collaborating administrations be managed? How should development measurement systems and administration of measurement campaigns in the context of net neutrality be organized in order to, achieve trust among stakeholders?

See answers above.

Question 2) Should measurement tools be based on Open source software? Which components could be Open source? What are the advantages/disadvantages of having an open source measurement tool? Who should have ownership over such measurement tools?

See answers above.

Security, reliability, availability etc.

Question 3) What security measures (individual or recurrent) should be put in place to ensure confidentiality, integrity (combating fraud) and the availability of measurement results and measurement systems? How should the system's software be updated?

> In cases where the individual user measurements are delivered to a collection server before the identifiable information is anonymised, the requirements for this server regarding security and oversight should be of an exemplary standard and comply with privacy,data protection and security-related laws and standards.

Question 4) If crowdsourcing is used: What should be the average monthly number of individual testers? What should be the average monthly volume of tests? What should be the profile of the testers? (i.e. geographical distribution, socio-professional, per operator, etc.) What means should be applied in order to ensure the representativeness of the panel of testers? (Commercial actions targeted, relationship with collectives, etc.) What post-processing should be applied to the measurements (reasons for exclusion of the results, etc.)?

See answers above.

System architecture aspects

Question 5) What kind of measurement system should be used and why: Environment dedicated to measurements (lines dedicated to the device)? Automatic measures by content and application provider sites (modules inserted in the source code of sites or applications trigger measurements when these are consulted)? Hardware probes (hardware dedicated to the performance of measurements or to the analysis of the user traffic connected to the user's point of access)? Measurement software (software which is installable on the PC or loaded onto the box, allowing measurements to be made)? Test of load on line?

See answers above.

Question 6) What type of measurements should be provided? What are the advantages and drawbacks of each type?

- **Active (i.e. traffic generated specifically for the performance of the measurements) or passive (i.e. observation of the user's traffic)?**
- **If active, should they be initiated (i) by the end-user or (ii) automatically (without the need for an action of the end-user)?**
- **If they are automatic, should they be triggered (i) locally by the client or (ii) remotely, at the request of the measurement server?**

NB. If your reply is dependent on the test carried out, please specify in which cases each indicator comes into question.

In addition to our previous explanations about active network tests, we want to bring to your attention an idea of one of our member epicenter.works about passive network testings which never made it out of a conceptual phase. While interesting, we experienced several concerns.

The TCP protocol offers statistics flags (performance counters)[9] for every connection. The collection of this information could deliver very accurate data about the real world performance of network activity[10]. Measurement tools could make use of these data.

The upsides would be:

- Instead of data about artificial measurements an overview about the performance of real user behaviour would obtained.
- The object of measurement is not changed by the measurement itself as it would by the use of active measurement processes.
- This measurement method is immune against distortion of the measurement by the isolation of testing servers from the actual network behaviour.
- Proprietary protocols (based on TCP) can be measured.

Downsides:

- Privacy problems with the collection about statistic/meta-data about user-behaviour. Potential solution: aggregate and anonymise the data as early and as thoroughly as possible (concentration points)
- Depends on adaptations on the client or server. (Theoretically, these statistic flags can be accessed on Windows and Linux.)
- Noise may be high due to bad user network connections (spotty WiFi, etc.), so long term measurements may be required.

Question 7) What should be the characteristics of the measurement servers? What are the minimum hardware characteristics to use the measurement tool? Where should the servers be located: In the operators' network? Among the hosts? In the Internet exchange points (IXP)? How should the choice of the servers be made? What should be the network connectivity of the measurement servers?

The measurement servers should be located in as many places as possible to gather measurement data as diverse as the real world user behaviour. A test which crosses the inter-connection point can gather information about increased packet loss which would indicate congestion and a potential inter-connection dispute. A test within a network could gather information about the specific traffic management practices in that network. Such a complete measurement suite would run tests against as many servers and against as many application-specific or throughput oriented measurements as possible. It might be advisable to seek out collaboration with CAPs and ISPs regarding the housing of measurement servers.

[9] https://www.ietf.org/rfc/rfc4898.txt (on Windows: https://msdn.microsoft.com/en-us/library/windows/desktop/bb485738(v=vs.85).aspx)

[10] https://technet.microsoft.com/en-us/library/jj574079(v=ws.11).aspx