Fédération des fournisseurs d'accès à Internet associatifs
(dite « Fédération FDN »)
FFDN — 16, rue de Cachy — 80 090 Amiens
Déclarée en préfecture de la Somme — W751210904

Answer to BEREC's stakeholder meeting in Brussels about net neutrality

Fédération FDN & La Quadrature du Net

March 14, 2017

This position paper develops the key points we exposed during a BEREC stakeholder meeting in Brussels. It is organized in topics, in the order in which they were discussed during the meeting.

1 Presentation

The "Fédération des fournisseurs d'accès à Internet associatifs" (Federation of the non-profit Internet access providers), also known as "Fédération FDN[1]", is gathering 30 non-profit Internet access providers, mostly in France, under its banner.

Each of these Internet access providers is managed by its subscribers. Each is also declared as an operator to the relevant NRA. Our operators are mostly established in France, including overseas, and one is established in Belgium.

The Federation itself is user-powered, all the actions being handled by volunteers, including this position paper. While it is written by volunteers, this does not imply they do not know very well the telecom market in France or in Europe. Our organisations are old (relative to the history of the Internet), and we have been working on these topics for many years. In France, the positions of the Fédération FDN on matters like net neutrality are considered serious, well-argued and have had an influence on policy-making. We do not usually act at the European level since it is quite difficult for volunteers to be present in Riga, Vienna, London or Brussels without significant funding.

La Quadrature du Net, an organisation defending civil rights and freedoms in the digital era, is working with us on this topic and position paper. La Quadrature has been acting at the European level since 2008. Its activity is focused on the empowerment of citizens regarding the defense of their rights and freedoms. The organisation produces analysis of legal texts, helping citizens understand them, and also develops tools helping citizens take action: following the work of the MEPs, for example.

[1] In reference to FDN, "French Data Network", a non-profit Internet access provider founded in 1992, which is the oldest Internet access provider still operating in France, and is the origin of our Federation.

2 Topic 1 – Measurement methodology / individual applications

We have a particular reading and understanding of the "closely monitor" question.

First of all, it cannot mean to monitor the network continuously, and without defined purposes. The same applies for a global monitoring of the network and, of course for anything regarding a given individual. Any systematic collection of data about the quality, speed, or operating state of the Internet access of an end-user must be regarded as attempting to her privacy: it *is* personal data. Even with a consent: everybody knows people "accept" every End User Agreement, without reading it. Some systematic measurements are interesting, as a global information, but nothing that could, by any mean, be used to attempt to the privacy of a citizen.

We do think a fine-grained measure, made on regular basis is way too damaging to a democratic society, even if the measure is based on consent.

Those global measures are, at least in France, already in place. They could probably be improved through several additions: knowledge of the interconnections between large scale network operators (ISPs, CAPs, CDNs, are all operating networks), of the rules applied to decide whether an interconnection agreement is allowed, of the saturation level of those interconnections, or of the difficulty to upgrade them. According to us it is not implemented enough yet. This information provides a clear view of operators abusing their position to try to gain un-deserved benefits.

E.g. if all the subscribers of an IAP want to access a given video platform, it seems reasonable that the video platform increases its capacity, investing in more servers, more content delivery networks, more content production, etc. Similarly, it also appears legitimate that the IAP invests to upgrade the interconnection to the content that its subscribers want to access since this is precisely what they pay it for. If it does not provide a good interconnection with services its customers want to use, this operator cannot be regarded as an "Internet Access Provider" but only as a "Local loop provider". The customer will then need to connect, through this local access, to a real Internet Access Provider. The typical way to achieve this is to use a VPN which grants access to the content through an encapsulated connection.

This global monitoring of the interconnections allows the NRAs to have a clear view of the playfield and identify both the operators which are willing to upgrade in good conditions their interconnection and the ones which are more reluctant to do so.

For individual services, we do not think it would be reasonable to have a systematic monitoring. This idea is, basically, that the quality of everything is always measured, and if the quality drops, there is a problem. We think the question should be turned the other way round. First we should get a detection of the problems rather than a monitoring of the quality. And when a problem is detected, then quality measurement can be used to provide relevant information.

For that detection, an open platform which collects individual reports, like Respect-MyNet (RMN, `respectmynet.eu`), is interesting. It allows to get information quite

quickly, and to investigate those reports. Campaigns to promote such crowd-sourcing information sites can help detect problems outside the realm of people specialised on networks. Such campaigns can be as simple as "You can access the service during afternoons, but not reliably on evenings? Please report." Another key point in the detection is that usually the infringement is publicly claimed by the perpetrator. The operators do **advertise about it**! They claim, on large ads in every place, that they have a specific offer to access a given platform or another. Last but not least, when infringements are not claimed, for example when an interconnection is overloaded every evening, the issue typically becomes public knowledge and everybody knows about it. Numerous reports are then received on public platforms such as RMN.

Real quality measurement can start once the problem is detected, in order to try to have a measure of it. The exact kind of measurement may vary (bandwidth, latency, jitter, DNS caching, packet loss, etc). But the idea is that once there is a suspicion, good and smart measures are possible. Those measures can be done with probes installed willingly by users: be they the ones reporting the issue or good-willing ones not specifically involved in that reporting. It is then easy to collate all the collected data into something coherent that can be easily interpreted.

If at the same moment a service is fluid for subscribers of operator A, slow for subscribers of operator B but not if these very same subscribers use a VPN to route their trafic through another path, then an interconnection problem exists.

Raw data collected during measures, made from individual lines, should **never** be published as-is. Such raw data contain PII and shall be subject to data protection rules. Data collection, processing and retention shall be done in line with GDPR rules under close control of the NRA and data protection authority. Only the aggregated results of the measure should be published. This means only publish the key values, without any possible way to get back to any individual behaviour. Moreover, investigation reports should probably always be published: an investigation was conducted about possible infringement on a specific case and it is of public interest to know it, even if the conclusion is that there is no infringement.

The kind of measures that can be useful in that context have already been exposed:

- same measures made from various places (same operator, or not, through a VPN, or not, etc);
- same measures made at different times (during night, on evenings, during day, etc);
- latency, speed, packet loss, in order to get the global network perceived quality;
- QoE (e.g. fluid video streaming, fluid download of an HTML page, etc);
- etc.

3 Topic 2 – Measurement methodology / IAS as a whole

The basic goal of that provision is to ensure that commercial advertising provides accurate information about the maximum available bandwidth for a given customer. The net neutrality issues are secondary for the question. The goal is to avoid advertising "up to 30 Mb/s" when your Internet access will actually provide 0.5M b/s. For the ancient technologies, like xDSL, the bandwidth is directly, physically, restricted by the landline itself; and sometimes also at some concentration point upper in the network. For recent technologies like fiber, the landline is not a restriction anymore.

Among the tests currently available, SpeedTest, the most widely-used one, is biased. Almost all large ISPs in Europe have an agreement with SpeedTest to host some of their servers. As a consequence, an end-user will only test his connection speed to the ISP's network. This helps ensure a higher result by getting the target of the speed measurement closer and located in a well connected part of the operator's network. We do consider this bias as acceptable in the context of this section. The speed measured is not really the bandwidth available for every usage of the Internet access provided by the ISP. But it is a correct measure of the specifics of the subscriber's landline, to compare against the landlines of others customers.

It can also be a valuable measure in network neutrality investigations. Example: the customer has 20 Mb/s available according to a SpeedTest-like measure, he cannot access a video platform in good conditions, and other customers of others ISPs with similar SpeedTest-like measures have good results. The problem is then not related to his specific landline, but to something in the network between his operator and the video platform: probably the interconnection.

A more technical measure that avoids the various environmental factors can be interesting as a diagnosis tool for the operator but not for the purposes of the BEREC. From a regulation point of view, a single poor measure may be due to poor quality WiFi and is not enough to bring to light a systemic network neutrality, or network capacity, problem. Of course, ISPs can use such tools to help diagnose their customer problems but BEREC should only consider the relative values between average customers on average landlines. For that matter, the environment factors are dissolved in the average: every ISP has its share of customers with poor WiFi. If an environmental factor creates a real difference on an average measure, the factor is then probably caused by the ISP (e.g. by providing very poor quality WiFi in the home-router that it lends or leases to its customers).

We would like to stress that everything cannot be measured. Some net neutrality infringement are simply decided in contracts with the end user. Some of the dispositions of such contracts do not respect the regulation for an open Internet. It does not appear as an achievable goal to make end-users *understand* the terms of their contracts and the law. Apart from those who know the law, they will *not* be proactive in reporting net neutrality infringements in their contracts.

Some ISPs within the EU are already infringing net neutrality, not only from tech-

nical measures taken by ISP, but also from contracts that do *not* respect the regulation and they will keep trying as long as they will be in a strong position.

4 Topic 3 – Practical considerations regarding implementation of QoS measurement systems

We do consider that the key point here is to protect privacy. These measurement probes will collect data about the behaviour of individuals in some circumstances. Some other aspects are also important, but this one must always be regarded as being the most important.

Technically, the measures are valueless if the measuring method is not properly documented from a scientific standpoint. Thus, according to us, it is required that the tools used are free software (and not merely open source). Free software guarantees three important benefits: that the tool will be used on all terminals, relevant, and that it will be trusted by end-users.

Merely opening the source code will eventually get some people to look at it, but as they won't be able to do anything with it in practice, it will give very poor results. Letting people look at the code and modify it ensures that opening the source is useful. Fostering a community by allowing feedback and code contributions to the tool means it stays relevant and up-to-date: if a new infringement is discovered, people can propose a probe that tests this infringement to the NRA. It enables faster iterations and ensures a wider variety of cases will be covered because the NRA is not the only one keeping an eye on the infringements to track.

It is also the only way to ensure that the tools will be available on any kind of terminal. The regulation states that the user can use the terminal of her choice. As a consequence, the tools used by NRAs and by the BEREC cannot create a discrimination between terminals. For these reasons, the measurement probe must be free software: open source, so that the exact description of the measurement mechanics is published; freely adaptable to any device or terminal; freely distributable so it can be available in any software repository for any end-user. A software that is only open-source would not be available everywhere (most Linux distributions, Replicant.us mobile phones, CyanogenMod phones, etc).

Another aspect to consideris trust. A probe that is installed on the end-user's computer must be a software that the user is confident with. If not, she will not install it. Free software allows that: everyone can see the source code, the users who can understand the code can explain what the probe does, and can tackle security issues, bugs, or unwanted behaviors. Being able to check if the software of the probe is not doing surveillance or sending data to a non-trusted organism is important and will bring trust. If the user is not able to do that, she will be reluctant to install and run a probe that makes measurements she cannot understand.

For every piece of software installed by the end-user, security is a key point. It is

not currently enforced by the various "Big data companies" which collect data with very poor security measures on the end-user side (see the various botnets built on IoT), neither on the central part of data-collection (see the various "hacking" reports in the news, with lot of data leaks of individuals). This project is in no way different. But since it is managed by a public authority, and an authority involved in the digital world, we do consider it is required to enforce those security questions, with a strict consideration for the security of the terminal, and security for the end-user and her privacy.

We think a modular approach may be interesting with a "core tool" to report measures and various probes that can be embedded in it. This makes it possible to add new probes on a regular basis and to have each probe make the appropriate measures needed by an NRA when investigating a supposed net neutrality infringement. It also allows the end-user to disable some probes when she thinks her privacy may be at risk. It will also foster a productive collaboration between NRAs and the rest of the world: the global tools being free software, any hacking, or activist civil society, organisation can provide new probes and integrate them in the core tool. This also requires that the data collected is in an open and documented format along with a documented structure (e.g. some JSON structure, documented), so that it is easy to articulate new probes with new data analysis.

As these probes should be free software, everyone will be able to contribute and develop a new module. This can be extremely useful: once a new kind of infringement appears, all the community can team up and propose a new probe to detect it. Such contributions might be made by insiders: people working for an ISP that is infringing Net neutrality and disapproving what is done can anonymously report the infringement or the infringement technique, providing the basis for the development of a new probe. Free software enables that kind of action.

We encourage BEREC to use its allies and protect them: contributing to the probes and to the report must be safe for them, as their are acting like whistleblowers.

We consider all data should be published. But nothing should allow any tracing back to the end user. There should be a clear documentation on how data are made anonymous by the system, and this documentation should be seriously challenged. It could become a reference on how to collect public data on people with no risk on privacy. There is probably a lot of space for a partnership with specialized researchers and scientific works on that topic: is the data really anonymous ?

The global and structural measures (interconnection links, over-capacity on the network, etc) are structurally anonymous (privacy is for humans, not for companies), and should be fully public. The user-centric measures, made from a private landlines, are subject to anonymization, and should be published aggregated.

Stating the obvious: the data published should be structured and usable data, publicly available without restriction or registering. Not a PDF file with the annual report.

5 Topic 4 – Net neutrality supervision tools and methods

We consider there are two very different kinds of infringements to the net neutrality.

The easiest infringement to detect are those made on a commercial basis. They are written in contracts, are usually displayed on large advertisement boards everywhere. The NRAs should read those contracts, and enforce the net neutrality rules. For example the zero rating (but other examples exist), which should be clearly forbidden, is at least in part controlled by the rules edicted by the BEREC. It is the responsibility of the NRAs to read the end-user contracts, check if it fits with the guidelines on net neutrality, and enforce them. We would consider it a failure to only stop the infringements: if there is no sanction, then there is no incentive for the ISPs to behave. The fact that NRAs can have different interpretation of the regulation and BEREC's guidelines is an issue. It does not enable a harmonized implementation of the regulation in all countries and leaves room for uncertainty for the end-users.

The complex part is related to the infringements made on technical basis. La Quadrature and some other NGOs have been developing for a long time a tool that helps the detection of problems regarding access to the Internet: Respect My Net (respectmynet.eu, RMN). It was designed from the very beginning to help the NRAs identify the problems, at least as they are perceived by the end-users across Europe. Such reports can be "there are 200 people saying that their Internet connection is poor with this video service on the evening", "there are 150 people saying they can't send emails" or others.

The project allows end-users to report different kind of problems encountered with their connection, and to « "upvote" similar problems if someone already did report what they witness. According to us, this kind of platform, available across Europe, can help the regulator track rumors of something going wrong: if RMN is showing a large number of people are having the same problem, it is interesting to trigger a targeted measure, and to publish the result of that investigation.

We consider that a tool which crowd-sources reports to detect the infringements, coupled with a general-purpose multi-probe measuring tool as described above, can be a very good way to detect net neutrality infringements. RMN is such a crowd-sourcing tool. Currently, it is developed by small NGOs, with almost no dedicated ressources, and evolves slowly. A coherent partnership between the involved NGOs and the BEREC, or the NRAs, can be a way to integrate that tool in a more formal process. Since this tool is managed by a cooperation of many NGOs, all across Europe, each NRA has a good chance to get reports from its local customers, in the right language and thus to create a better interaction.

The same tool, developed in a top-down approach, from the Commission, to the BEREC, to the NRAs, etc, would probably be far less efficient, using a lot more ressources to produce a result poorly adapted to the differences of the various European cultures. It seems more efficient to have a good interaction between the civil society organisations that created the tool, and the NRAs, that use it. NRAs could, for example, provide information on the kind of infringements they would like to detect, or

provide some evolutions on the tool (helping the localisation effort, for example).

Having a common platform in Europe will also help the different NRAs coordinate and compare their situations, at the BEREC level.