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 public consultation on its guidelines to enforce Net Neutrality in Europe

Fédération FDN

July 18, 2016

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 federating 30 non-profit Internet access providers, mostly in France.

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 the response to this consultation. While this response is written by volunteer people, 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 Brussells without significant funding.

2 General considerations

2.1 On the consultation process

The draft guidelines have only been published in English, the consultation itself is in English, and the various statements from BEREC about the way to submit answers to the consultations suggest, more or less clearly, that any answer not written in English faces a serious risk of not being read or taken into account.

[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.

This consultation is, supposedly, not only aimed at the corporate lobbying from the largest operators in Europe, who can all easily deal with technical and legal English documents. It is supposed to be open to civil society, emerging businesses, or small operators, whether those are businesses or non-profit organisations like ours, and of course to the citizens.

The guidelines are a technical document. It requires specific skills to be read. Skills about technical matters, of course, but also skills about European legislation, and about the telecom Regulation it does implement. The fact that it is only available in English adds an additional barrier to an already challenging consultation. We do clearly consider this as an hostile position from BEREC, trying to keep the small actors out and trying to protect the *entre soi* of the large corporations.

We do also consider it as a kind of dereliction towards European citizens, who have been involved in the legislative procedure, working with the European Parliament to support and enforce net neutrality in Europe. Claiming to open the consultation to "all stakeholders" with a consultation only available in English is from our point of view opposed to the European spirit of "united in diversity", and a way to try to restrict the consultation to "all shareholders". Not the same citizens, not the same Europe.

BEREC is composed of 28 NRAs. Each NRA is skilled enough to translate the consultation from BEREC's working language to its national language, and to translate back the answers, or a synthesis of those answers.

2.2 On the regulatory approach

BEREC has, in several portions of its text, a reflex that consists in waiting for the regulation to be circumvented, then think about that case, and only afterwards act on that specific case and possibly create a rule about it. This typically is the position of BEREC on zero-rating. This is dangerous for two reasons. First, it leaves such cases in a grey area. Second, it is based on the assumption that the market is doing good by itself, which is a quite hazardous assumption to make.

We know, and understand, that this is the usual regulatory approach: wait for something to happen, and once proved the open market will not fix by itself the damages it caused, create new constraints on the market to fix the problem. The Regulation at hand has been written by the Parliament, the Council and the Commission precisely because the damage is now clearly identified, and because it has clearly been identified that the open market *will not* automatically protect net neutrality.

It should then be the role of those guidelines to state clearly which practices are acceptable and which practices are off-limit. The whole "grey zone" of malpractices that will be analysed *ex-post* is a resignation of BEREC, who refuses to undertake its duties.

3 Application of the Regulation

About paragraph 4. The approach of BEREC, stating that *end-users* are individuals & businesses, sounds fine to us. The same rules should apply to the Internet access of every end-user.

But size does matter: large organisations can do more damage, and so must be more controlled. Great power comes with great responsibilities, as the famous quote goes. When behaving as end-user, a large scale platform powered by a large organisation creates a risk by itself, that an individual does not create.

They are both allowed the same access to an open Internet, and the same right to provide applications and content, but large corporations have more strength to ensure its rights than the average individual or very small businesses. The NRAs should then have in mind that providing the same rule is not efficient *per se*. It also requires a more protective behaviour towards small businesses and individuals.

The purpose here is to define that individual end-users have the same rights than large companies using the network, on which we do agree. But large companies have ways to "negotiate" with their ISPs: when a large bank is dealing its IAS, it has more weight in the commercial transaction than the average individual end-user. So, a practice that can be acceptable for large companies (say, creating an incentive but not really blocking) must be considered aggressive toward individual end-users.

If one needs to call the customer support to be able to "provide applications and services of [his] choice" (Recital 7), it is not a problem for a large company, yet it is practically ensuring it will not happen for the large majority of individual end-users.

NRAs should take great precautions when analysing the specifics of a market, to ensure that the end-users rights are enabled *by default*, without requiring a lot of actions from the individual end-users. NRAs *may* accept solutions a bit more demanding for large companies.

So we propose adding something like "But, since CAPs, and more generally end-users who are large companies, have a better leverage when negotiating commercial agreements with their ISPs than the individual customers do, the NRAs will ensure that the rights entitled to individual users are not folded in complex rules designed for the CAPs and professional consumers".

About paragraphs 10 to 12. Geographical coverage area

A Wifi network in a restaurant, a Wifi network covering a village, and a Wifi network covering students residence halls all over France are all the same technology, but with a different geographic reach.

Our estimation is that it is more about the "purpose" than the geographic coverage or the technology used:

- Wifi in a café: it is for the private "domestic" use of the customers, so extremely close to a normal IAS, it is not a tool for the café or the restaurant to do its business (like is a coffee machine) but something offered to the customers for their usual normal usage;
- Internet access in a company: it is for the company's own good (even if sometimes used by employees to check their private e-mails), so very different from a normal IAS. The Internet access here can be considered like any tool in a factory, its purpose is not to provide Internet access to the employees, but to provide a tool for the company;
- Internet access in a students' residence hall: it is their Internet access in their rooms, obviously private domestic use, the same as would be an Internet access in any other place, apartment, house. On the other hand the access in the classrooms is something totally different, closer to the Internet access used in a company, its purpose is then to be a teaching tool.

So we do consider the approach of BEREC in paragraphs 10-12 to be slightly wrong. The question is not about the size of the coverage zone, neither is it about the technology. The question should be about the purpose, i.e. the targeted normal use of the access.

If the Internet access provided in a café *may* be slightly different, it is because it is only provided very temporarily, for a few minutes to a few hours, and so some distinctions may be acceptable. For example, a public IP address allowing the customers to provide applications and contents from their laptop while in the café may be regarded as not required, the lack of public address being acceptable. But content filtering, or allowing only websites having partnerships with the café, is not acceptable.

We do consider that the two main points here are the purpose of the IAS, and the stability of the contract. If the purpose is to provide Internet access to the individual, and on a long term basis, then it is an IAS as described and protected by the Regulation. If it is in a very short term contract, like is the Wifi in a restaurant, then some elements of the Regulation may not be relevant. And if it is a tool used in a company, it is not an IAS for the employees, it is an IAS for the company, and so the Regulation does not apply to protect the employees (but some other rules still apply, like privacy and correspondence) but to protect the company which is the end-user.

If the IAS is not regarded *per-se*, like in a company, then the "responsibility shift" cannot be presumed. Since the access is potentially restricted, filtered, controlled, managed, etc., then, the company is *still* responsible for what the IAS is used for. On the

contrary, an ISP is *not* responsible for what its customers are doing. This point is, for us, a clear consequence of the status and rules applied to ISPs: they do provide open Internet access to citizens (or organisations), empowering them, and leaving them liable for their own doings. A company providing filtered Internet access to its employees is not in the same position, and thus should not have the same protections.

About paragraph 16. IPv6 is required for end-users to provide content and applications. The Regulation's implementation as a whole suggests that it is not the case and is wrong in this regard.

In more detail: to be allowed to provide content and applications, the end-user must have a public address provided on her IAS. There is no more IPv4 addresses available, and soon it will be impossible to provide one to everybody. Major ISPs are already refusing to provide public IP addresses along with their mobile Internet access, which is a problem for net neutrality.

Soon, because of the exhaustion of IPv4 address, the only public IP addresses available will be in IPv6. And so providing public IPv6 addresses to end-users will become mandatory to satisfy the Regulation.

Another approach is to consider the new-comers. ISPs have a stock of available IP addresses, and this stock is large enough for their day to day use for still some time. But new comers will not get a lot of IPv4 addresses (see the various RIPE reports on IPv4 exhaustion and allocation strategy). It will then create a huge barrier for new-comers if IPv6 is not widely used and available.

About paragraph 17. We do **strongly** support this approach and analysis.

Sub-Internet can clearly be used to circumvent the Regulation. The NRA analysis should clearly avoid that. The approach proposed in the first version of the BEREC guidelines, as submitted to public consultation, is the only decent position possible.

4 23-26. About terminal equipments

About paragraphs 23 to 26. As the Directive 2008/63/EC defines "terminal equipment" as "equipment directly or indirectly connected to the interface of a public telecommunication network", here, the equipment can be seen either as a computer or a phone, for example, connected to a network, or as the so-called "box[2]" provided by many French ISPs: the home-router installed by the ISP in the user's home to give him easy access to the network.

The first case states the obvious: the terminal is under the user's responsibility, thus he has the right to choose. We do support that position. The terminal is part of the

[2]On the French market, since 2002, the word "box" is used to name the home-router, and/or the TV set-top box, or any kind of integration of those two (e.g. Livebox, Freebox, etc.).

domestic installation of the end-user, and should be under his decision and control — just like on the water network the faucet in your kitchen is yours to choose.

In the latter case, we support BEREC's position that the end-user has the right to replace the equipment provided by the ISP by another of her choice, when it is not proven that the equipment provided by the ISP is technically required. ISPs often use such equipment to propose other services to the user (e.g. games, online data storage, replay TV, video on demand, etc), making the home-router a powerful tool for bundling other services and creating a captive market. We suggest the NRAs to make clear that the final equipment can be mandatory only if there is a valid technical reason, and only if the equipment is restricted to that specific purpose.

For example, on a cable network, the specific modem configured with the "golden frequencies" of the network operator may not be available on retail (golden frequencies cannot be setup by the end-users of that kind of system). In such a case, the modem itself is required for the network access. But it should not be bundled with a home-router creating other constraints.

The specific use of an IAS by an end-user is shaped by the routing system she uses: most of the routers provided by ISPs are designed to easily *use* applications and contents, they are not designed to easily *provide* applications and contents (e.g. working only in NAT mode as a router, and not in bridge mode to allow the public IP address to be directly on the PC). And the Regulation states clearly that any end-user has a right to distribute (or use) the information, applications and content of her choice. Thus, the end-user has a right to choose her equipment.

The notion of network/equipment compatibility applies on two ends of the domestic terminal. One end is the network: technological compatibility (frequencies, color for the fibre, kind of modulation for DSL, etc). This end is under the control of the ISP. The other end is the equipment which has the public IP address, and is seen on the Internet. This one must be under the control of the end-user, as explained above. The split between those two realms is clear: the required equipment provided by the ISP should offer standard interconnection (like, say, gigabit Ethernet) and standard protocols to setup the network (e.g. DHPC or PPP) so the end-user can use any home-router she may choose.

The home-router, integrating the network access part with some routing capacities (Wifi network, domestic router, etc) can be proposed to the customer *only* if it can be turned to a single bridge device (allowing the user to have her own routing device), or if a single bridge device is available at no extra cost.

There should be some elements about those points in the guidelines, stating the clear limit on the part of the domestic installation that the end-user can choose.

5 Zero rating

About paragraph 32. We do support the approach exposed in this paragraph. Our organisations consider it implies the total ban of zero-rating from Europe. Any form of zero-rating. Despite the paragraph is unfolding the arguments in the reverse order, it exposes clearly that a data-cap, or speed-based pricing, when applied in an agnostic way, abides by the net neutrality principle. The counter-point is then that a limitation (speed, volume), when applied in a non-agnostic way, *per se* harms end-user rights.

Zero-rating, whatever the approach, is a differentiation in traffic types. Per definition: if some traffic is zero-rated, everything else is not. So it is structurally not agnostic. It could be application-agnostic, but not agnostic. Even an open approach stating "there is a data-cap for video streaming, and no limit for everything else" can hardly be regarded as valid.

First, it cannot be regarded as technically justified: if data volume is consuming resources on the network, then the kind of data is not relevant. Second, it promotes some kind of usage (passive consumption of video content) over others (like providing content, or providing applications, or interactive chat with other users), which goes against the freedom of choice of end-users.

The approach exposed in paragraph 32 is simple and straight: speed and volume limitation are conform to the Regulation when they are agnostic. It is the only approach that can be supported.

About paragraph 33. In the case described in this paragraph, only the *subscription* of the service is bundled with the subscription fee of the mobile access. Meaning it is only a commercial transaction, with no effect on the network, or on the mobile access *per se*. Meaning the data-cap of the mobile access subscribed is not concerned by the bundling, and the data included in this data-cap is not concerned by the bundling. Under those clarifications, we do agree with the approach provided by the BEREC.

If the bundling also includes privileged access, or not counting the access to the bundled service in the data-cap, then, it *must* be regarded as an infringement under paragraph 32.

Anyway, such a bundling will also be checked against the more general rules applicable to any market, such as "tying", so that the very same mobile access should be available without the bundling of the music service, and the music service should be available without the mobile access.

It should also, of course, be considered under other applicable laws. The service known in France as "SFR-Presse", which bundles together an IAS and a subscription to online newspapers, can be considered a problem. It creates a strong incentive for IAS customers to read some politically-oriented news titles (*Libération*, part of the same industrial group, is considered to be pro-government, left-oriented, information press). Everyone in France knows that it is made for tax purposes. VAT on press subscription is 2.1%, while it is 20% on IAS. Claiming half of the subscription to the IAS is related

to the press subscription is clearly for tax optimisation. But this tax optimisation has a very strong effect on the society as a whole. It is a way to use a strong position (being the second largest ISP in France) on a market to create a strong position on a very sensitive market: the news media.

This is why, during parliamentary work on the Regulation, the proposed approach was about controlling whether ISPs's handling of information flows had a constraining effect on society, or if they enabled a free society to grow and develop. Part of this is still present, in a tempered manner, in the Regulation. In recital 3 of the Regulation one can read "The existing regulatory framework aims to promote the ability of end-users to access and distribute information or run applications and services of their choice.".

Net neutrality, and market regulation, are tools aiming to ensure end-users can access the information of their choices. When an ISP uses its central market position to impose, through whatever means, technical or commercial conditions introducing a significant bias in the way users will access information (especially information of the most sensitive kind like political news), this must be regarded as a very clear contradiction to the goals of the Regulation and to the goal of ensuring media pluralism laid down in paragraph 43 of the guidelines. Consequently, such price-based discrimination must be considered by the NRAs as a great damage to the principles underlying the Regulation.

About paragraph 39. The global analysis of that paragraph is the one we also adopt in our answer to paragraph 33. Unfortunately, there is no conclusion in paragraph 39. It describes the zero-rating of non-application-agnostic traffic as being an incentive to use this service rather than that of a competitor. But it lacks the obvious conclusion: this kind of zero-rating is *not* allowed by the Regulation, as stated by paragraph 32. Here the BEREC is cowardly trying to avoid applying the Regulation as clearly wished by the European Parliament.

A bout paragraph 42. "Materially" in the last sentence should be "Practically" (i.e. in practice) as stated in the Regulation.

One can "materially" drive a car without a safety belt. One almost never "practically" does it. Thus, the rule enforcing the use of safety belt is effective.

Similarly if the ISP's behaviour leads to end-users "practically" not using their rights/choices despite being "materially" allowed to do so, it should be regarded as an effective limitation of those rights, and so prohibited by the Regulation.

About paragraph 45. Regarding items 2 and 3: if a higher price is considered as invalid in respect of the Regulation, then a lower price should be invalid too, and even more so a zero-price. Higher or lower must be analysed in the same manner here.

Point 4 must be considered as a clear rejection of zero-rating, in coherence with our reading of paragraph 32.

6 Quality of service, network management, advertised speed

About paragraph 47. This paragraph is unclear to us. The interconnection, or more specifically the poor quality of the interconnection, can damage QoS. If the ISP provides a good interconnection to his own service, but very poor interconnection with his competitors; or if he refuses to setup the same quality of interconnection with two competing services, it creates a technical difference in quality between the two applications/services.

It should be the role of the NRA to control whether those interconnections are fair or unfair. Unfair interconnection rules can be a way to discriminate contents or applications, even under article 3(3).

Since all of this is obvious, the meaning of paragraph 47 is unclear. It may be considered as stating that an interconnection between two operators (ISPs or others) should not be regarded as an end-user IAS, which is also obvious.

About paragraph 61. The last sentence, stating that encrypted traffic should not be treated less favourably for the sole reason of being encrypted, is something important. It is of course stating the obvious, at least for people who have some knowledge in matters like computer security or privacy. But because it is not always obvious for people less know-how on these issues and considering that encryption is extremely important for security and privacy, we want to stress our clear and strong support for having a dedicated paragraph about this issue.

About paragraph 75. As for technical neutrality, the blocking performed in the network at the request, and under the control, of the end-user, can be considered to be "terminal equipment based". It can be a good way for users to protect themself from many things (e.g. blocking spam). It is acceptable for such filtering to be performed at the network level rather than on terminal equipment (so, saving some data transfer from her data-cap for a mobile access, for example), as long as the user can efficiently manage this filter, as she would on his terminal.

The point is not where the filtering is performed, but where and by whom it is controlled. So we do insist strongly on "under the control of the end-user". During recent discussions at ARCEP in preparation of this draft of the guidelines, it was one of the points getting a clear and loud agreement from all stakeholders (large operators, small ones, civil society, etc) that having things under the control of the end-user should be the priority, so as to promote greater control of the end-users on their online life.

About paragraphs 89, 113 & 114. We do support that approach on congestion. If the network does not have enough capacity, then the IAS must be preserved, and the specialised service may be turned down.

About paragraph 164. Lacks a closing parenthesis on 5th line, but who cares?

7 Enforcement and NRAs means of action

In the enforcement part, we are quite surprised to find a very loose frame around NRAs means of action to deal with the cases to be raised on the matter of net neutrality. We identify two problems: firstly, the Guidelines say a lot about what NRAs *can* do but little about what they *must* do. With such an approach, NRAs will be encouraged to do the very minimal amount of work to enforce the Regulation. Given the reluctance of the biggest actors on this market to respect net neutrality principles, NRAs must be in position to force them to protect their end-users' rights, with the adoption of proportionate sanctions against offenders when necessary. In order to protect the end-users effectively across Europe, the Guidelines should be much stricter on the enforcement role of NRAs, and how they are to proceed against various instances of net neutrality violations.

Secondly, the guidelines fail to plan for a cross-European warning mechanism. How will the NRAs coordinate to harmonise their responses to the different cases that will arise (with, for instance, an observatory listing the cases already known and the actions taken to address them)? The risk here is having at the end of the day every NRA trying to deal with its cases without noticing the others, with a high probability of producing conflicting case laws in EU member states.

Moreover, there are still too many questions which are not addressed. Some are easy ones, like the procedures to be used by the citizens to protect their rights, the kind of organisation that can start the procedure. What will be the NRAs methods and powers to investigate, and to ensure appropriate actions are taken when a net neutrality problem arise?

The NRAs are going to produce, in Europe, some legal precedents on this new kind of litigation. Will it be available in all the languages of the Union, like is the ECJ jurisprudence, or only in English like this consultation? Who will ensure those precedents are made coherent across Europe, and how? Is it a part of the "law", enforcing the rights of the citizens, that cannot be easily accessible to the citizens?

The annual reports made by each NRA, giving this kind of case law on the NRA's decision, will probably be consolidated in an annual BEREC report on net neutrality. Will all of that be published? Will it be subject to consultation? Will all the documents be only available in English? How can the citizens access the knowledge base about their rights?

If a NRA is not willing to apply the Regulation, what will happen? If a decision made

by a NRA is not conform to the guidelines, what will happen? What is the procedure for citizens, and for civil society organisations, to act when a NRAs is failing its duties?

In fact, all the questions about how will the citizens know their rights, and what they can do to protect them, are not handled at all in the guidelines. And these questions are important.

8 On empowering end-users

We support BEREC's will to encourage "user-level assessment" (paragraph 170) of IAS' performance, and to "empower end-users" (paragraph 137).

Recital 3 of the Regulation notes that "a significant number of end-users are affected by traffic management practices which block or slow down specific applications or services", but today, only users that already have technical knowledge can do something because they understand how Internet works and what measurements to perform is appropriate. All the other end-users are totally needy on this point. Even if they suffer from a very serious infringement on net neutrality done by their ISP, they have absolutely no mean of action. End-users need to be armed and BEREC can help on this.

"Empowering end-users" by clarifying the terms of the contract between them and the ISP is a good start, but it is not enough. We need users to be able to understand what is a net neutrality infringement (at least the basics), so as to produce relevant data and raise cases, at the European level, for example via a platform like `https://www.respectmynet.eu` (built by civil-society NGOs) and simple measuring tools — like RTR-Test `https://www.netztest.at` (built by the Austrian regulator). In fact, part of this work is already done, but it could benefit from more institutional support and needs more European coordination (so as to have measurements that are comparable at the European level, for instance).

Measuring the quality of the connection[3] is a good tool for this: only with good measurements at hand users can address themselves to the NRA and prove the problems on their connection are due to a net neutrality infringement. Because there is objective data. If the tools producing the data are transparent and understandable, that's even better.

We think BEREC has a good opportunity here to help the member states' NRAs apply the Regulation (more cases will be raised) and to have comparable data at the European level. This goes totally in the direction of "data-driven regulation" as promoted by ARCEP: documenting cases on a single platform helps the regulator to keep track of issues and needs on the market.

[3] By "quality of the connection", we understand not only the speed or latency measurements (quality of the link between the Internet and the end user), but also its quality in the meaning of the Regulation: is a port blocked, is an application unusually slow, etc. In short, is there a violation of net neutrality.