November 4, 2019

Comments to the Draft BEREC Guidelines on the Implementation of Open Internet Regulation (BoR (19) 179) (1)

Executive Summary

Overall, the regulation overplays the importance of traffic management, i.e. quality of service but ***tends pay little or no attention to the role of security***. The text seems to assume that ISP network implemented security could be used to defeat the purpose of the regulation and therefore ISP implemented security is to be avoided. This is like saying that guns should be banned because they can be used to kill people. It is reasonable to adopt a more refined attitude to security because the lack of security is the biggest problem for users of Internet access services. The regulation should further assume that hacking activity with the goal of taking control of user devices in continuous and automated and that known vulnerabilities when found will be utilized by the hackers. In the 5G era, hacking on the Internet that is connected to the physical world is a matter of national security of the member states. This regulation should not create obstacles to improving internet security and national security as a result.

If treated properly, security services could be a new revenue source for the ISPs without sacrificing any of the goals of the regulation for equal treatment of services and applications. This is because security is an area with a huge shortage of skilled labor in Europe. The situation demands large scale automation of the provision of security services. A key role in this automation naturally falls to the ISPs and their cloud platforms that are now emerging due to 5G, virtualization of network functions and the Software Defined Networks. Instead of restricting the ISPs from taking that role, the regulation should encourage the ISPs to seek new entrepreneurial approaches to provide better security to their end users. It will then be the task of the NRAs and this regulation to make sure that security processing is not used as an excuse to implement business practices that defeat the purpose of this regulation.

When the ISP invests into the cloud platform, ***this regulation should not disfavor the ISP or MNO to make the best use of that platform as compared to cloud services providers***. This is justified by

- Fair treatment of different players on the same market. If e.g. MNOs are restricted to implement some 5G functionality using the “compute” elements in 5G, existing cloud provider will gain new business turf from 5G.
- The fact that the ISPs under this regulation are European companies while most cloud services providers at the moment are global (near-)monopolies like AWS, MS Azure, Google and Facebook. From the European perspective it is not reasonable to open any new opportunities to these global companies while restricting European competition to them. New business turf will be opened by new technology such as 5G. The question is who will occupy that new turf. The non-European global near-monopolies or the European network

operators. If the latter, BEREC and EU will have leverage over what kind of business practices are established for the new turf for example in matters of protecting the citizens' privacy. In case the new turf, in particular, on the boundary of the physical and digital worlds will be occupied by the US cloud companies, the power of BEREC or EU as a whole in for example matters of protecting the citizens privacy will be limited or non-existent. This would be a huge loss for the European citizens and a threat to the national security of the member states.

- To provide cost efficient services, the ISPs and MNOs are moving to use virtualization (i.e. cloud platforms) to implement the networks themselves. Full cost savings similar to cost savings in IT services due to cloudification are possible only in case the ISPs and MNOs are allowed to make the best use of the new platform. Any limitations on the ISPs and MNOs to use the cloud platforms will mean higher cost of future services, lower and slower adoption rates of the future services and the EU being left behind China and the US in the new services.
- The cloud platforms of the ISPs/MNOs allow to implement completely new types of services if the services are out of scope of the Open Internet regulation just like cloud services are now out of scope of this regulation. The ruling that ISP/MNO cloud platforms would be out of the scope of the regulation will not need to weaken customer choice or fair treatment of applications or OTT services in any way. On the contrary, this will increase customer choice while weakening the possible interest of the ISPs to get involved in commercial practices that this regulation tries to restrict.
- Possible customers to ISPs/MNOs of their cloud service include Content Distribution Networks (CDN) such as Akamai or Over-the-Top (OTT) providers such as Netflix. Those now are allowed to bring their computer racks to IAS premises and make shared operation arrangements for this hardware. This works for large IAS. It does not scale to small IAS. This favors the large companies and raises barriers of entry to telecoms markets. This barrier could be lowered if the small (and large) local IAS would be allowed to rent its virtual machine capacity to the OTTs and CDNs. Another possible customer, naturally, is the MNO/ISP subscriber/end user.

In addition, the regulation should take care to offer the ***same opportunities to both fixed network ISPs and Mobile Operators***. If for example it is possible to provide parental control to fixed line subscribers, it should be possible to do the same for mobile customers. The current version does not allow the same opportunities to mobile as it offer to fixed networks. This idea is aligned with technology neutrality stipulated in the draft guidelines. A technology neutral ruling is easy to implement in the text by separating the concepts of Network Termination Point (NTP) of the Mobile Network from the NTP of the internet and focus in this regulation on the Open Internet rather than "Open Mobile Network" which now happens by accident when the MN air interface is used as the NTP for mobile users.

Detailed comments

Article 2. item 12, recital 4 has the text:

points of the internet. Providers of internet access services should therefore not restrict connectivity to any accessible end-points of the internet.

The above statement is problematic because it is in conflict for example with the common and popular practice of Network Address Translation (NAT) in the mode “address and port dependent mapping and filtering” (APDMF). Such NATs will allow client end points to access services on the Internet but the NAT applies filtering in the reverse direction such that responses (or response lookalikes) from all other sources except the one earlier identified by the end point in a request message with Address and Port number will be filtered out or dropped by the NAT. The above statement implies that an IAS could not use this NAT mode on its network e.g. in a Carrier Grade NAT.

An alternative to APDMF type NAT would be e.g. Endpoint Independent Mapping and Filtering. Such a NAT opens all ports of the client to all other endpoints while the Mapping is active. If applied to e.g. Mobile users, this would mean that the air interface and an actively communicating mobile device would be exposed to all malicious endpoints connected to the Internet. This would require some serious firewalling on the battery powered device and still an attacker could deplete the device battery easily with a low intensity attack. This battery depletion attack is not possible if the NAT used by the MNO is of APDMF type.

To solve this issue, the minimum correction is such that endpoints are classified to those with globally unique addresses and those with private addresses and that the currently widely used practices related to NATs are permitted. A more generic correction is also possible. Because a NAT is really a type of simple Firewall, let’s look at the statement from this angle.

More generally, the statement forbids network-based Firewalls or blocking services operated by the ISP. It may, for example, be known to the ISP that an endpoint has been proven to be a malicious web site that distributes viruses. Corrective action may be ongoing with the help of the ISP. But for the time the corrective action has not been completed, it is clear that access to the site should be restricted to the purpose of the corrective action while normal use of the web site should be blocked.

To remedy this flaw, the minimum correction is to add to the end of recital 4 “except for security reasons”.

This would be a sufficient remedy also for the NATting issue as explained above.

From a wider perspective, all kinds of NATs are necessary for the current Internet. A NAT is a simple Firewall. Its normal operation is such that endpoints with a private address are not reachable by unsolicited flows from other end points while initiation of outbound communication from a NATted address works fine. Administrators like NATs because they allow to hide the end points from malicious attacks that are continuously ongoing and run by automated hacking software. Also, NATs extend the IPv4 address space. So, we MUST allow NATs. Then the question is why should other kinds of network-based Firewalls be banned? There are good grounds to claim that this is not technology neutral.
For more generic network-based firewalls, vertically integrated products do not allow to give sufficient control to the end user of the Firewall operation. With the introduction of virtualization, this will change.

Article 3

> Recital 5
> When accessing the internet, end-users should be free to choose between various types of terminal equipment as defined in Commission Directive 2008/63/EC (1). Providers of internet access services should not impose restrictions on the use of terminal equipment connecting to the network in addition to those imposed by manufacturers or distributors of terminal equipment in accordance with Union law.

The network technology is offering a new opportunity for the end users: they could rent a virtual machine (VM) on the ISP/MNO platform to carry out some processing of the traffic to and from their other terminals. This is most relevant for small companies that, for example, could run their network firewall on the ISP cloud platform in immediate proximity to the attachment of the company internal IP network to the ISP network. Some small companies may rely entirely on the mobile network and have no fixed network at all. It should be possible to build network firewalling functions on the MNO cloud platform for such small companies. Reasonable goals of the placement of the firewall is to minimize delay and energy consumption by minimizing the physical route the company packets must travel. In 5G era, this goal is best achieved by using an ISP/MNO cloud platform. Same kind of processing can become reasonable for the consumer end users as well simply because it is technically feasible to isolate a VM on the cloud infrastructure from all other VMs and the users have unfulfilled security processing needs. Technically, there is nothing stopping the ISP/MNO renting VMs to its own subscribers to meet the end user needs.

It is not reasonable that this regulation should limit the way ISPs can make commercial use of their cloud platform: the ISPs should enjoy the same opportunities as the cloud services providers that are out of scope of this regulation.

Several different business models are used by the cloud providers such as IaaS (infrastructure as a service). This would correspond to an arrangement where a small company rents a VM or several VMs from the ISP/MNO and either by itself sets up its Firewall in those VMs or delegates the technical setup and maintenance to a security intelligence company that will use those VMs to provide the service.

An alternative is that the VM capacity on the ISP cloud platform is sold as PaaS (Platform as a Service). In that case the ISP would offer the VMs together with some platform Software to the subscriber. The subscriber would then obtain, install and use the rest of the needed Firewalling Software and make the needed arrangements with a security intelligence company. Finally, the ISP/MNO could offer the cloud service to its subscribers as Software as a Service (SaaS). In this case all the firewalling software would be provided in the package.
Under the SaaS model different arrangements for security intelligence provision and managing the firewall rules are possible. The normal market economy rules will make sure that the ISP has no leverage to use these arrangements to limit the customer choice in any way: the users and subscribers will buy such value-added services only if the services meet their needs and they are happy with them. Nor is it economically feasible for the ISP to use this arrangement to disadvantage some services or applications for commercial gain. Such attempts could also be explicitly forbidden by the regulation. For the time being, buying into these services would be entirely optional for the end users and subscribers. From a technical perspective making such firewalling compulsory would be reasonable for careless users who have been detected to have

hacked devices in their networks and who have failed to restore security in their devices. If BEREC however feels that commercially, and legally this would be a hard ruling to move forward, in this regulation any compulsory application can either be ruled out or left of NRAs to decide for further experimentation on the market.

In the world and in particular in EU there is a huge shortage of security experts leading to low level of security in many companies that cannot afford to hire real experts on network security. Also security expertise of ordinary consumers leaves a lot to be desired. The other way to look at this shortage of skilled labor is that the productivity of the existing experts should be increased. In other areas of IT than security, the answer to increasing the productivity of the IT experts has been the move of lots of IT applications and services to the cloud where the level of automation can be hugely increased as compared to managing the services and applications on physical computers or scattered devices. It is reasonable to expect similar gains in productivity in the area of security if computer security processing for end users could be widely moved to the cloud. A key role in such a move naturally falls to the ISP/MNO that has to invest into cloud technology for this role in the best location e.g. for 5G networks. It is not reasonable to limit the ways that investment can be leveraged to improve the end user services so long as the offerings by the ISPs will improve the services to the end users and thus improve the customer choice.

Further on in item 25: we have

> *"Use terminal equipment of their choice"*
>
> 25. Thirdly, end-users have the right to use terminal equipment of their choice. Directive 2008/63/EC defines *"terminal equipment"* as *"equipment directly or indirectly connected to the interface of a public telecommunication network"*. The right to choose terminal

In light of this regulation, for cloud services providers a VM is equal to a physical computer. This should be the case also for subscribers of IAS services.

If the VM rented by the user or subscriber from the ISP/MNO cloud platform is placed on the customer side of the NTP of the internet, the VM fulfills the above requirement. This very placement is also optimal in terms of delay and energy consumption in providing e.g. firewalling services. Therefore, it is reasonable to amend the item 25 with this VM option.

Article 3 (2) 32a has the text

Examples of such additional services are parental control services and filtering services provided via secondary DNS resolvers, HTTP proxy and access router/modem-based functions on end-user side of the network termination point[13].

This guideline, may be seen to limit the choice of technology or cause a lack of technology to achieve a certain goal such as "parental control".

The real dilemma of a parent is that all members of the family may have several devices in use, many of them wireless or mobile. No single box at home can control the use of those devices. In particular, a mobile device does not rely on any additional routing/switching nodes at home (on the customer side of the air Interface which in the current version is the NTP). The best way to scale the parental control to all the devices the children have is by implementing the control on

the MNO cloud platform. In such a solution, the same rules can apply equally and fairly to all children of the family if that is what the parent wants. Naturally, it must be the parent, not the MNO who defines and manages the rules. With the earlier technology of vertically integrated boxes giving such control to a subscriber has not been feasible. Now with the use of virtualization of computing (cloud technology) this has become possible for an ISP/MNO.

In "BEREC Guidelines on Common Approaches to the Identification of the Network Termination Point in different Network Topologies" (2)

Item 141 it is defined that in mobile networks the NTP is on the *air interface*. In the introductory part of (2) it says that the document defines what is a network termination point (NTP) to the public communications network. The regulation (1) does not take into account that in case of mobile we have **two independent public communications networks**: (a) the mobile network (MN) and (b) the internet which from the point of view of MN is the Packet Data network (PDN) for which the MN provides a "virtual wire" connection. As a result, the regulation at hand ***does not allow implementing parental control for mobile devices***! This puts mobile network operators at a disadvantage against fixed network operators. Nor does the regulation allow implementing cloud-based Firewalling for small companies that rely on mobile network only on the MNO platform. This violates against the Recital 2 in Article (1) of the regulation at hand that requires that regulation is technology neutral.

If for the purpose of this open Internet regulation, we would clearly separate the two networks: MN and the PDN=internet with their completely separate NTPs, all would be logical and well and unfairness of the current draft would be removed.

Just prior to the point of attachment to the Internet, the MNO could route the packets to its cloud platform where the parental control or firewalling could be implemented just on the customer side of the point of attachment (where among other things the publicly visible IP is assigned to the mobile user packets) i.e. the internet NTP. This kind of approach would also be true to how the fixed and mobile networks really work and would fairly compare the fixed and mobile networks. It would clearly stick the regulation to its stated scope which is open Internet and not "open mobile network!"

One could claim that for commercial purposes MN is a part of the Internet. However, this does not work. It would then follow that e.g. base stations and other MN infrastructure elements are just like routers and visible on the internet. This is not the case. Those elements belong to a private network owned by the MNO. If they would be on the internet, they could be attacked from consumer devices with poor security that would work as a botnet. Facilitating this kind of attack is not acceptable and would lead to a completely unpredictable quality of service for the mobile users. Also, protecting the air interface – a valuable commodity – from attacks requires that we keep MNs private rather than a part of the internet.

The Guidelines at hand deal with the Internet. It would make sense to say in Article (1) that the *Guidelines (1) do not limit the way a mobile network is implemented and that the MN is seen as a "virtual wire" to the internet that is the scope of the regulation while MN as a whole is out of scope. One could then say that the implementation of the virtual wire shall not defeat the purpose of this regulation.* For the MN this is no hardship because the MN does not look inside the IP packet that it carries over its packet transport network and that outside the MN will be carried over the internet, not to talk about the payload of the IP packet. This way, the MN is under the umbrella of the guidelines but its regulation does not go into any details of the implementation of

the MN. The guidelines should limit themselves into defining the minimum properties of the "virtual wire" provided by the MN in such a way that goals of the regulation are fulfilled.

End user rights Article 3 (2) items 34 - 48

No provisions have been made on ***obligations of the end users or subscribers***. It would seem reasonable to state that the connected devices of an end user or subscriber have no rights to cause harm to other connected users or device owned by other users. If the end user has connected to the internet low security devices that are abundant on the markets and/or has been careless in configuring his/her devices, they can be hacked and overtaken by malicious entities and used for malicious purposes against other users of the internet. The value of the damages from hacking is estimated to be Billions of € every year.

It would be reasonable to rule that the ISP is allowed to use its best efforts to identify and constrain it's served devices that are used in malicious activity. In the current practice in many countries this kind of activity is taking place under the guidance of the National Cyber Security centers or similar. Moreover, it would be only fair that the ISPs would be allowed to gain some revenue from such efforts which is however not the case at the moment. It would be reasonable that an EU level regulation would allow NRA's to experiment in this area.

Moreover, it would seem reasonable to rule that the end user should apply his/her best efforts to either remove from the internet or restore to a benevolent state the connected devices that its ISP has identified to the user as being participating in malicious activity. Moreover, the subscriber should be obliged to remedy his/her devices in a way that they cannot be hacked again as soon as they are reconnected to the Internet. It should be assumed that the hacking activity on the internet is continuous and automated. As a result, most known vulnerabilities on devices will be found and utilized by the hackers.

It would be reasonable to allow the ISP to block internet access to malicious devices that the end user has not corrected irrespective of the guidance given by the ISP.

Article 3(3) first subparagraph, item 53

> Thus, even though packets can experience varying transmission performance (e.g. on parameters such as latency or jitter), packets can normally be considered to be treated

The excerpt mentions "packets". It should be understood that a packet network such as the internet treats all packets based on its instantaneous load situation. So, all packets are treated differently. Talking about equal treatment is technically meaningful only for either (a) the algorithms the network node uses to process the packets or (b) for some packet aggregate such as a flow, service or application. Since (a) cannot be observed externally, it is wise to concentrate all regulation to (b) where statistics can be collected on the connected devices and the fact of equal or un-equal treatment can be established based on the statistics data.

For this reason, it is wise to keep the talk about packets to a minimum in this regulation. Mentioning such generic measures of QoS as "packet loss" should be permitted because it can be measured on an end-to-end connection.

Article 3(3) second subparagraph

> be transparent, non-discriminatory and proportionate, and shall not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic. Such measures shall not monitor the specific content and shall not be maintained

This statement can be understood to be more restrictive than the new text in Article 3(2) item 34a that allows QoS mechanisms that are application agnostic. A reasonable clarification is that the idea of QoS that is application agnostic and under user choice is repeated here and that the "objectively different technical quality of service requirement" case is clearly limited to the case where the *ISP has judged* that a certain application (such as voice) objectively needs a certain quality of service and will take traffic management measures on its own discretion.

Such a correction would improve the clarity of the Regulation (1).

In the same Article **Recital 9 has the text**: "Such measures should not be maintained for longer than necessary."

It is the nature of all reasonable QoS mechanisms that they do not waste network resources. If objectively different types are assigned different QoS classes, then it is reasonable that this classification is for the long term and will stay in force until the NRAs and the ISP make a new judgement on the matter. For these reasons, *the above sentence in the recital is unnecessary*.

In the same Article there is a text:

> Recital 10
> Reasonable traffic management does not require techniques which monitor the specific content of data traffic transmitted via the internet access service.

It would reasonable to add a clarification to the end "more than is necessary to identify the objectively different types of traffic".

Item 71-73 are not needed. This comment is the consequence of our earlier comment on Recital 9. The items just clutter the text without adding clarity.

Article 3(5) first subparagraph

> **Article 3(5) first subparagraph**
>
> Providers of electronic communications to the public, including providers of internet access services, and providers of content, applications and services shall be free to offer services other than internet access services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality.

The need for *specialized services* often arises due to high security requirements that cannot be met by internet services. By isolating a specialized service such as communications for Smart Grid

from the internet altogether it will be possible to make DDoSing or attacking the service infeasible using the typical methods that are used by the hackers or disgruntled teens. In such solutions, remote access to the service can be best arranged using the mobile networks without sacrificing security.

So, for clarification purposes appending the above with “level of quality **or security**” would be helpful.

For example, in items 106 - 112, the assumption is that specialized services are about the QoS while the consideration of security is left without attention. The security requirements of use cases are typically independent of the bandwidth or other transmission characteristics of the underlying network technology and will remain invariant while it is possible to connect unsecure equipment to the internet.

Item 115 – VPNs. It would be wise to say that this regulation does not limit the choice of technology that is used to provide security for the network-based VPNs while such technology is not used to defeat the purpose of this regulation.

Acknowledgements: Several people in the Finnish 5G Research community and professor Petri Mähönen of RWTH have commented on this contribution and encouraged to submit it.