Implementation of EU Net Neutrality rules: safeguarding end-users' rights in Internet access services while promoting innovation and user choice

1. Introduction

The European legislators have now adopted the Connected Continent Regulation establishing new rules on net neutrality ('the Regulation'). Cisco, Ericsson and Nokia believe the political compromise reached by the European legislators struck a reasonable balance between protecting rights of end-users of Internet access services and ensuring freedom to continue to innovate and develop new services.

However, whilst the political process is over, the next steps of implementation and bringing the regulatory framework into force present an equally important part of the policy-making process. The BEREC guidelines will be an essential part thereof to make sure the new rules become operational and are applied in a consistent manner across the 28 Member States. To become operational, some of the concepts introduced in the Regulation need further clarification to provide the necessary legal certainty for providers of electronic communication services to the public as well as providers of content, services and applications, in particular as concerns the provisions on services other than Internet Access Services (non-IAS services). As technology enables new types of services, creating richer experiences for all users, enabling industry to stay competitive and the public sector to deliver better services to its citizens, our networks and the traffic on them becomes much more diverse. In turn, managing these networks, and regulating them, becomes correspondingly more complex. As we look to implement the new net neutrality rules in Europe this comes to the fore; whilst the Regulation seeks to protect end-users' right around the provision of one specific electronic communication service, namely Internet Access Service (IAS), networks are already used today to deliver a variety of other electronic communication services and will deliver even more in the future. BERECs guidelines should take particular care to ensure that the Regulation will be innovation friendly and that the ability of networks will continue to be of value into the distant future in delivering services, content and applications with the choice of Service Level Agreements (SLAs) and quality of experience customers wish. BEREC should turn to the work done so far by industry associations and standard bodies when it comes to traffic management rules and how they are implemented.

2. Non-IAS services

The Regulation states clearly that providers of electronic communication to the public and providers of content, applications and services are free to offer services 'other than Internet Access Services' (non-IAS): *(**emphasis** added)*

> *"Providers of electronic communication to the public, including providers of Internet access services, and provider of content, applications and services shall be **free to offer services other than Internet access services**..."* (Art. 3(5))

This is in line with the objective and scope of the Regulation, '*to safeguard equal and non-discriminatory treatment of traffic in the provision of Internet access services*'. Consequently, while the provision of non-IAS services is subject to two important safeguards vis-à-vis users of IAS, the Regulation does not regulate non-IAS as such.

2.1 Safeguard 1: Non-IAS not used to circumvent IAS provisions in Art 3(1) to (4)

The first safeguard seeks to ensure that IAS cannot simply be re-packaged as non-IAS service by establishing that the optimisation is necessary to deliver the specific level of quality:

> *"...services other than internet access services which are optimised ..., where the optimisation is necessary in order to meeting requirements of the content, applications or services for a specific level of quality."* (Art. 3(5))

> *"There is demand on the part of providers of content, applications and services to be able to provide electronic communication services other than internet access services, for which specific levels of quality, **that are not assured by internet access services**, are necessary."* (Recital 16)

> *"The national regulatory authority should verify whether and to what extent such **optimisation is objectively necessary** to ensure one or more specific and key features of the content, application or services and **to enable a corresponding quality assurance to be given to end-users, rather than simply granting general priority over comparable content**, applications or services available via the Internet access service and thereby circumventing the provisions regarding traffic management applicable to the Internet access service."* (Recital 16)

As clarified by the Commission in a statement made to Coreper upon approval of the political agreement[1], this is a safeguard to ensure that the provision is not

[1] See annex

used to circumvent the traffic management rules in the provision of IAS and inter alia the paid prioritisation ban. Consequently, necessity should be measured against the demands of the end-user purchasing the service and the ensuing need of the provider of the service to ensure delivery to the specified and contractually agreed level of quality. It is also clear that the non-IAS offer has to be considered with respect to the IAS service characteristics that are available at the time and place as well as the content for which the non-IAS service is intended to convey. It is clear that different services will offer IAS with materially different characteristics, especially as between wireless based and fixed connection based services. Furthermore, the characteristics of both IAS and non-IAS services can be expected to vary over time as both content and technology changes.

For instance, imagine that a consumer wants to be able to access audio-visual content with guaranteed HD quality and availability with fast channel change. The consumer's IAS provider offers, through a commercial deal with a content provider, a VOD or IPTV service with specified quality attributes in the contract. The consumer purchases this service from his or her ISP in addition to the Internet access service. For the ISP to be able to deliver this service, the ISP will need to optimise the transmission of traffic for this service (provisioning, mobilising network resources, securing delivery…). Thus, the optimisation is from a technical point of view '*objectively necessary*'.

The guidelines should incorporate the European Commission's statement attached to the Regulation and thereby clarify that the safeguard against circumvention of Art. 3(3) should be ex post and necessity assessed in consideration with the end-user requirements and the provider's ensuing contractual obligation to deliver the enhanced level of quality.

2.2 Safeguard 2: Sufficient capacity and no negative impact on the general quality of Internet access services

The second safeguard seeks to ensure that the provision of services other than IAS does not have a negative impact on the availability and general quality of IAS:

> '*Providers of electronic communications to the public, including providers of internet access services, may offer or facilitate such services only if the network* ***capacity is sufficient*** *to provide them in addition to any internet access services provided. Such services shall not be usable or offered as a replacement for internet access services, and* ***shall not be to the detriment of the availability or general quality of internet access services*** *for end-users.'* (Art. 3(5) second subparagraph)

In order for this safeguard to be effective in practice, the BEREC guidelines should provide further details on how this is to be interpreted and enforced.

We contend that the first step to make it operate in a manner which protects users of Internet access services and at the same time enables innovation is to interpret 'sufficient capacity' in conjunction with 'general quality of Internet access services.' In other words, there is no requirement in the Regulation to establish ex ante that the electronic communication services provider has sufficient capacity to provide services in addition to IAS. As long as such services are provided without detriment to the general quality of IAS, it should be deemed that there is sufficient capacity. The mix can vary over short periods of time and any ex-ante determination is unlikely to be proportionate. Instead what matters is the on-going time averaged general quality of IAS. This is particularly the case of wireless services.

Secondly, 'general quality' cannot be determined in a vacuum or in a 'one size fits all' definition. The general quality safeguard should be assessed in view of the objective of the Regulation and the related end-user rights in relation to IAS, i.e. the appropriate transparency requirements around the transfer speeds communicated to users (Art. 4(1)d). This should also take into account the increased simultaneous use of an Internet connection as households include an ever-increasing number of connected devices.

Thus, insofar as IAS end-users are experiencing speeds within the range advertised and as contractually agreed, the provision of services other than IAS by the same telecommunication service provider of the IAS should be presumed to be in compliance with the general quality safeguard in Art. 3(5).

Both the expectation and performance may legitimately be different from one network to another. Further, it will vary over time and with technology used by the provider. In practical terms, it is unlikely for a regulatory authority to be able to monitor every provider in terms of the technical characteristics listed in the recitals at a reasonable cost. A practicable alternative would be to require that providers can demonstrate, with technical evidence that no degradation has occurred whenever a complaint arises. The need to make suitable measurements is a normal expectation of such undertakings and the obligation to provide evidence should not represent a large additional burden. Regulators should avoid the temptation to provide benchmarks that might have the effect of removing technical competition from the markets. Equally, the significant measurements may vary from one network to another and forbearance is needed to avoid regulation from adversely affecting competitive choices by operators.

Further, it should also be clarified in the BEREC guidelines that 'general' quality implies an element of quality 'on average' or over a certain period of time, implying that non-IAS may have a temporary impact on the availability of the IAS.

If for instance an IAS end-user also purchases a home automation and security solution, including video security, from the IAS provider as a non-IAS service and in the event there is a burglary, the video transmission will be prioritised ahead of other traffic, potentially having a temporary impact on the availability and quality of other IAS end-users. The implementing guidelines should make clear this level of impact is still within the bounds of the Regulation. As it is difficult to predict traffic volumes notably in mobile networks, as recognised in recital 17, the impact of non-IAS on IAS may be particularly unavoidable. The guidelines should reflect that.

2.3 Electronic communication services outside the scope of the Regulation

The Regulation applies to providers of Electronic Communication Services (ECS) to the public, including providers of Internet access services. This limitation of scope to electronic communication providers to the public also applies to the Regulation's non-IAS provision:

> '*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…*' (Art. 3(5))

This also follows from the objective of the Regulation, to safeguard end-users' interests around the provision of Internet access services:

> '*This Regulation establishes common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights.*' (Art. 1(1))

As such, private networks fall outside the scope of the Regulation. However, already today there are plenty of ECS being provided which are services that could be interpreted to be non-IAS as described in the Regulation, i.e. services which are optimised to deliver specific levels of quality and service, but which are not provided to the public.[2] This will be even more the case in the future as more and more business, industries and cities become connected. The BEREC guidelines should provide clear recognition of the distinction between ECS and

[2] As defined by the EU telecommunications framework Directive, an ECN is public if provisioned wholly or mainly for the purposes of offering publicly available ECS. Thus, if the ECN is provisioned wholly or mainly for the purpose of private communications, it is a private network.

ECS *to the public* to avoid the Regulation is not unintentionally extended to also cover what will essentially be private networks.

Such networks and services are for instance a connected factory, a smart city or a connected retail centre where the network is not available to the public, even if the network is provisioned and managed by an Electronic Communication Network (ECN) provider that may operate *other* networks, which are open to the public. As 'what goes on within that network, stays within that network', there can be no negative impact on any Internet access services which the ECN provider may be providing on its publicly available network and therefore the guidelines should recognise that such networks fall outside the scope of the Regulation.

This also encompasses the cases in which such private networks may be providing a Wi-Fi access to its users, for instance a connected port, which offers Wi-Fi to its employees and users, or a smart city[3], which provisions part of its network for a Wi-Fi service to its citizens. There mere fact that such a network provides Wi-Fi access does not change the fundamental private nature of the network as such Wi-Fi access will only be ancillary to the primary purpose of the private network, i.e. the network would still not amount to a publicly available network as it will not be wholly or mainly provisioned for offering publicly available ECS. The networks in the above examples will primarily be provisioned for electronic communication services within in the private network, e.g. in the port example this will be logistics, security, back office administration. Equivalently, a smart city's network is mainly for the purpose of enabling smart parking, smart waste, connected street lights etc.

This also entails that as these private electronic communications networks are dimensioned to deliver private electronic communication services, it is often the excess or spare capacity, as it exists from time to time, which is used to provide Wi-Fi. Consequently there is no agreement in existence between an end user who is a member of the public and the proprietor. Therefore a smart city, connected port and similar cannot be seen to become providers of electronic communication services including of an Internet access service. There is nothing in the regulation that indicates that it was the intention of the authors to curtail such services. Article 14(6) of the original Commission proposal supports this interpretation. The article was deleted when the Parliament and Council decided to focus the Regulation specifically on roaming and net neutrality, but gives the

[3] Smart city: "A smart city is a place where the traditional networks and services are made more efficient with the use of digital and telecommunication technologies, for the benefit of its inhabitants and businesses.", see European Commission https://ec.europa.eu/digital-agenda/en/smart-cities. Examples of smart city projects include cities such as Amsterdam, Barcelona and Copenhagen.

best indication of the political intention, stating: "An undertaking, public authority or other end user shall not be deemed to be a provider of electronic communications to the public solely by virtue of the provision of public access to radio local area networks, where such provision is not commercial in character, or is merely ancillary to another commercial activity or public service which is not dependent on the conveyance of signals on such networks." The BEREC guidelines should confirm this to ensure the Regulation cannot be interpreted in a way that could stifle such provisions.

Another important service, which BEREC should provide guidance on, is a virtual private network (VPN) service. As the name indicates VPNs provide a functionally equivalent of a physical private network but where the customer purchases the VPN as a service from an ECN provider. VPN services will differ depending on the different customer needs and can be delivered in different ways, e.g. they can be delivered over a leased line or on a non-IAS. Whether they offer site-to-site or network-to-network connectivity, VPN's typically carry only the traffic to reach devices, computers and servers connected to the remote site or network. In VPN's the topology of the virtual network is not constrained by the access tails or the manner in which they are implemented. What is common to all VPNs is that they have SLAs and that they provide a cost-effective and scalable alternative for businesses and other private and public sector organisations to establish a private and secure communication network.

The VPN will as recognised by the Regulation in most instances also provide access to the Internet:

> '*However,* ***the mere fact that corporate services such as virtual private networks might also give access to the internet should not result in them being considered to be a replacement of the internet access services****, provided that the provision of such access to the internet by a provider of electronic communications to the public complies with Article 3(1) to (4) of this Regulation, and therefore cannot be considered to be a circumvention of those provisions.*'
> (Recital 17)

The BEREC guidelines should make clear that it is only as far as the Internet access service is concerned that network and traffic management is limited to the provisions in Art. 3(1) to (4) and thus the electronic communication network provider offering the VPN service is able to implement the network and traffic management tools necessary to deliver the service levels specified in the relevant SLA. Further, the guidelines should clarify that this does not hinder the customer of the VPN to implement any user policy towards the users of the Internet access services, usually employees, within its organisation. It should be noted in this regard that while the Internet access service may provide access to

virtually all end points on the Internet, subject to any organisational policy, it will still not be an Internet access service for the purposes of the Regulation as it is not publicly available; it is only accessible to a pre-determined group, e.g. company employees, and it is delivered via a network, the VPN, which is not wholly or mainly used for the provision of publicly available communication services but used to provide for secure corporate operations. As such, VPNs are an extension of the corporate network using technologies such as firewalls, filtering, blocking, to provide security for the corporation.

3. Traffic management for Internet access services

The Regulation clearly recognises the role of reasonable traffic management as an inherent part of delivering Internet access services and to ensure an efficient use of network resources without this being in contradiction to the principle that all traffic should be treated equally:

> *'**The first subparagraph shall not prevent providers of internet access services from implementing reasonable traffic management measures**. In order to be deemed to be reasonable, such measures shall 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 for longer than necessary.*' (Art.3(3) subpara 2)

Importantly it recognises that differentiated traffic management plays a positive role in managing increasingly complex networks and types of data and traffic flows as long as equivalent types of traffic are treated equally:

> '*The requirement for traffic management measures to be **non-discriminatory does not preclude providers of internet access services from implementing**, in order to optimise the overall transmission quality, **traffic management measures which differentiate between objectively different categories of traffic**.*' (Recital 9)

This explanation of non-discriminatory is essential to include in potential further detailed implementation guidance.

Besides the further specific comments below, where we do not believe the Regulation is sufficiently clear as to what the intention is and where the unclear wording could lead to inconsistency in interpretation, we believe the principles established around what constitutes reasonable traffic management are

generally sound. There are however numerous ways in which to implement traffic management; broadband networks use different network architectures and access technologies which may require different approaches to traffic differentiation. The Regulation and the guidelines should not limit different approaches as long as such approaches comply with the principles that the traffic management and differentiation is based on the objective, technical requirements of the traffic within that class. It should be made clear that a class relates to market substitutes and not to a class defined in any standard or recognised specification. For further reading see for instance a non-exhaustive list of traffic management tasks with examples of use cases and links to technical implementations described in the *Technical Report TR-134 Broadband Policy Control Framework* from the Broadband Forum organization[4], Bitag (2015): *Differentiated Treatment of Internet Traffic*[5] and Predictable Network Solutions Ltd (2015): *A Study of Traffic Management Detection Methods & Tools*[6].

New methods of traffic management may come with Software Defined Networking (SDN) and Network Functions Virtualization (NFV), which are generating significant interest in the telecommunications industry due to the promise of creating flexible networks, making them more dynamic and responsive while providing operational benefits. BEREC's guidance should not be too specific on the technical means to leave space for innovation.

3.1 No monitoring of specific content:

Another criteria for reasonable traffic management, which should be further clarified in the implementation guidelines is the prohibition of monitoring specific content. This criteria is not defined in the articles themselves nor explained in any further detail in the recitals which simply states:

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

It is presumed that the provision only concerns reasonable traffic management, i.e. that it introduces a ban on monitoring for purposes of ensuring packets arrive at their destinations at the right time. This however would need to be clarified in implementing guidelines to ensure the provision would not come to prevent operators from gathering information, i.e. monitoring, for purposes of technical and customer support issues, forensic analysis, security and statistics.

[4] https://www.broadband-forum.org/
[5] http://www.bitag.org/documents/BITAG_-_Differentiated_Treatment_of_Internet_Traffic.pdf
[6] http://stakeholders.ofcom.org.uk/market-data-research/other/technology-research/2015-reports/traffic-management

It is also the case that in some instances the appropriate class of traffic handling for a packet is not apparent from the header alone. It seems appropriate that the class be determined wherever it is found and that the requirement not to monitor applies to taking summaries and recording rather than determining packet treatment for each packet. It would seem that the monitoring element is related to the prohibition in 3(4) on processing of personal data but clarification is needed if we are to prevent unintended consequences of inadvertently hindering otherwise permitted reasonable traffic management.

3.2 These measures may not be maintained longer than necessary:

The reasonable traffic management provision also states that such measures may only be maintained for as long as necessary. Again this provision in the article is not further explained in the recitals but simply word for word repeats the wording in article 3(3) subpara 2:

> '*Such measures should not be maintained for longer than necessary.*' (Recital 9)

The potential issue with this rule is that it implies traffic management is something switched on and off. As it is not expected to be the intention of legislators that operators constantly have to change the configuration of their networks, the implementation guidelines should clarify that this means networks should not be configured in a manner which maintains the effect of traffic management for longer than necessary.

The guidelines should also include a clarification that some types of traffic are normally given special priority based on their traffic type, such as VoIP, and it is necessary for as long as the traffic type uses an IAS. It is quite common for such long-lived applications to need special treatment continuously for periods of years. Such services are indeed what was intended to be permitted and not prevented by the architects of the regulation. It would be unfortunate if a too-literal interpretation had the unfortunate outcome of stopping VoIP from working in the open Internet and in VPN access tails.

3.3 Interplay between reasonable and non-reasonable traffic management

In addition to the provision on reasonable traffic management the Regulation also introduces a ban on blocking, throttling, slowing down etc. of specific content, applications and services:

> '***Providers of internet access services shall not*** *engage in traffic management measures going beyond those set out in the second subparagraph, and in particular shall not block,* ***slow down****, alter, restrict, interfere with, degrade or discriminate*

between ***specific content, applications or services, or specific categories thereof,***' (Art. 3(3) subpara 3)

However, as the provision covers not only measures against specific content etc. but also categories thereof and also covers a much wider range of actions, including slowing down, it should be clarified in guidance that slowing down refers to the overall transmission rate at which such packets are forwarded and not the delay incurred by individual packets. It should also be clarified that packet dropping is implicit and the slowing down refers to dropping at differential rates compared to the overall volume on a link. Otherwise there is a risk that the distinction becomes blurred between reasonable traffic management, where differentiated traffic management between different traffic classes is permitted, and traffic management beyond this reasonable management only permitted under narrow circumstances.

One general comment on packet loss as relates to it being used as a QoS parameter in recital 17, it is important to understand that packet loss is not necessarily a "bad thing". In fact, when buffers overflow they will drop packets to ensure the traffic flows more smoothly. The dropped packets will often be re-sent automatically within seconds or milliseconds. If the buffer on the other hand does not drop packets, it can start to cause congestion and delays. NRAs should therefore be careful not to draw wrong conclusions from higher levels of packet loss. Dropped packets also provide a method of applying fairness to prevent users of very fast sources from blocking capacity to others. Great caution needs to be taken in specifying any limits which are couched in technical terms which might not be universally translated into consumer outcomes.

For further information, please contact:

Cate Nymann
Manager, Government Affairs
Cisco
+32 (0)495 27 9886
cnymann@cisco.com

Walter van der Weiden
Director, European Affairs
Ericsson
+32(0)496 86 2233
walter.van.der.weiden@ericsson.com

Florian Damas
Director, Government Relations
Nokia
+32 (0)477 96 0544
florian.damas@nokia.com

Annex: Commission statement following Coreper approval of political agreement on 8 July

COMMISSION'S STATEMENT

"The Commission explained that in its view neither Article 4 nor Recital 11 of the agreed text of the draft Regulation introduces a special authorisation regime (i.e. different from the general authorisation regime under the Authorisation Directive). Article 4 states that NRAs shall closely monitor and ensure compliance with Article 3, and thus requires NRAs, as part of their ongoing monitoring activity, among others, to verify compliance of services other than internet access services, which are optimised for specific content, applications or services, with the criterion that such optimisation is objectively necessary and not a circumvention of the provisions regarding traffic management applicable to the internet access service. Article 5 states that Member States shall lay down penalties applicable to infringements of Article 3 and shall take all measures necessary to ensure that they are implemented. The NRA powers to take measures to ensure compliance with this criterion will therefore include where necessary the power to impose dissuasive penalties."