Barbara van Schewick
Professor of Law and by Courtesy, Electrical Engineering
Helen L. Faculty Scholar
Director, Center for Internet and Society

November 28, 2019

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

I welcome the opportunity to comment on the Draft BEREC Guidelines on the Implementation of the Open Internet Regulation. I submit these comments as a professor of law and, by courtesy, electrical engineering at Stanford University whose research focuses on Internet architecture, innovation and regulation. I have a Ph.D. in computer science and a law degree and have worked on net neutrality for the past nineteen years. My book "Internet Architecture and Innovation," which was published by MIT Press in 2010, is considered the seminal work on the science, economics and politics of network neutrality. My papers on network neutrality have influenced discussions on network neutrality all over the world.[1] I have testified on matters of Internet architecture, innovation and regulation before the California Legislature, the US Federal Communications Commission, the Canadian Radio-Television and Telecommunications Commission, and BEREC.[2] The FCC's 2010 and 2014 Open Internet Orders relied heavily on my work. My work also informed the 2017 Orders on zero-rating by the Canadian Radio-Television and Telecommunications Commission, and the 2016 Order on zero-rating by the Telecom Regulatory Authority of India. I have not been retained or paid by anybody to participate in this proceeding.[3]

My comment draws heavily on my existing writings on net neutrality. The papers most relevant to this consultation are attached to this submission. I would welcome the opportunity to discuss these important issues further.

Interactions between Art. 3(3) and Art. 3(2)

Relationship between Art. 3(3) and Art. 3(2) (para. 37)

Para. 37 of the draft guidelines rightly clarifies that "[n]either the rights as set out in Article 3(1) nor the requirements of Article 3(3) can be waived by an agreement or commercial practice otherwise authorised under Article 3(2)."

---

[1] See, e.g., van Schewick (2007); Frischmann & van Schewick (2007); van Schewick (2015b).
[2] See, e.g., van Schewick (2008); van Schewick (2010c); van Schewick (2010b); Federal Communications Commission (2014).
[3] Additional information on my funding is available here: http://cyberlaw.stanford.edu/about/people/barbara-van-schewick.

This clarification is necessary and important. In recent years, ISPs have argued that Art. 3(2) should be interpreted to allow end users to waive the protections in Art. 3(1) and Art. 3(3) by entering into agreements with their ISPs. This interpretation would fundamentally change the character of the regulation and allow ISPs to do an end run around the regulation by including blocking or discrimination in the contract with the user.

The ISPs' interpretation has shown up in two variants: First, ISPs have argued that traffic management measures associated with zero-rating plans should not be subject to Art. 3(3) as required by the current version of the guidelines. Instead, traffic management measures associated with zero-rating plans should only be evaluated under Art. 3(2). Such an interpretation would allow ISPs to technically treat zero-rated content differently from other content, for example by limiting the amount of bandwidth available to zero-rated products, but not to others. We saw this with T-Mobile's StreamOn offering that originally throttled video from participating providers to 1,7 Mbps. German telecom regulator Bundesnetzagentur found this to be violation of Art. 3(3), since it treated zero-rated video different from content, applications, and services not participating in the program. The decision has since been upheld by the Higher Administrative Court of Münster.

Second, beyond zero-rating, ISPs have argued that Art. 3(2) allows them to block or discriminate against content, applications, or services by including those practices in the contractual agreement with the user. For example, an ISP could block all online telephony services as long as this is specified in the contract.

The draft guidelines rightly reject the ISPs' interpretation. The interpretation in the draft guidelines is required by the wording of the relevant provisions, the goal of the regulation, and the history of the regulation.

First, the wording of Art. 3(1) and Art. 3(3) makes clear that both provisions apply to any offering of internet access service and are mandatory in nature. The prohibitions on blocking, discrimination and other technical practices in Art. 3(3) applies to ISPs "when providing internet access service." The words "shall treat all traffic equally" in Art. 3(3), subpara. 1 or "shall not block, …, or discriminate" in Art. 3(3), subpara. 3 show that this requirement is mandatory. The exceptions to the ban on blocking etc. in Art. 3(3) third paragraph are clearly enumerated in a-c, and the language introducing these exceptions ("except as necessary … in order to") suggests that these are the only exceptions to this requirement that the regulation envisages. Allowing commercial agreements between ISPs and their end users to override the obligations under Art. 3(3) would also be impossible to square with Art. 3(3) subparagraph 2, which clarifies that reasonable technical traffic management measures shall not be based on commercial considerations.

Second, this interpretation is also required by Art. 1(1). According to Art. 1(1), the "regulation establishes common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services." Thus, the requirements in Art. 3(1) and Art. 3(3) are explicitly referenced as key goals of the regulation, suggesting that these provisions are the

cornerstone of Europe's net neutrality regime. By contrast, the ISPs' interpretation would allow ISPs to nullify these critical parts of the regulation through the backdoor of Art. 3(2). Thus, the ISPs' interpretation of Art. 3(2) would effectively allow ISPs to "circumvent provisions of the regulation" – resulting in exactly the outcome that, according to Recital 7, Art. 3(2) was designed to prevent.

Third, the ISPs' interpretation cannot be reconciled with the history of the regulation. Allowing ISPs to legitimize blocking or discrimination by including such practices in the contract would re-establish the net neutrality regime that was in place in Europe before the adoption of the regulation in 2015. Under the old regime, ISPs were allowed to block or slow down traffic as long as they disclosed it to their consumers. This regime lead to widespread blocking and discrimination, disclosed in contracts. For example, many ISPs prohibited and blocked the use of online telephony services, or limited the amount of bandwidth available to peer-to-peer file-sharing applications during times of congestion. These practices motivated the European Union to adopt explicit net neutrality protections against blocking and discrimination.[4] This history is explicitly referenced in Recital 3, Sentences 3 and 4.[5] Thus, the ISPs' interpretation would effectively re-create the regime that the regulation was explicitly designed to end.

In line with these insights, Art. 3(2) allows ISPs and customers of their IAS to contractually agree on technical conditions and technical characteristics of the service that do not violate Art. 3(3), as long as those agreements do not limit the exercise of the rights of end users under Art. 3(1). The technical practices associated with such agreements still need to comply with Art. 3(3). Art. 3(2) does not allow users to contractually waive an ISP's obligations under Art. 3(3) or Art. 3(1).

This interpretation leaves ample room for agreements under Art. 3(2) without neutering Art. 3(1) and Art. 3(3), which are key parts of the regulation.

The examples of "agreements on commercial and technical conditions and the characteristics of internet access services" provided in Art. 3(2) support that interpretation. While agreements on "price, data volumes or speed" might involve technical restrictions, the technical restrictions necessary to implement them to do not violate Art. 3(3) because they do not differentiate between applications or classes of applications. Data caps limit how much data an end user can use overall and the plans might limit the amount of bandwidth available once a user reaches their cap, but these limits are application-agnostic – they apply to all traffic equally and do not differentiate among applications or classes of applications. Similarly, providing internet access service with a contractually agreed upon maximum speed (e.g., up to 1,5 Mbps) involves technically limiting the amount of bandwidth available to a user to 1,5 Mbps, but does not

[4] See blog post by Kroes (2012).
[5] Recital 3, Sentences 3 and 4: "However, a significant number of end-users are affected by traffic management practices which block or slow down specific applications or services. Those tendencies require common rules at the Union level to ensure the openness of the internet and to avoid fragmentation of the internal market resulting from measures adopted by individual Member States."

discriminate among applications or classes of applications and therefore does not violate Art. 3(3). Similarly, charging a higher price for internet access service with a higher speed or a higher cap does not involve distinctions among applications or classes of applications.

Thus, Art. 3(2) allows agreements and commercial practices that do not violate Art. 3(3), either because they do not involve technical measures that would be subject to Art. 3(3) or, if they do involve technical measures, these measures do not violate Art. 3(3). An example of the first case would be zero-rating certain apps without treating them technically different from apps that are not zero-rated; an example of the second would be agreeing on technical characteristics or technical conditions that are application-agnostic. As discussed below, in addition to agreeing on speed or volume caps, allowing ISPs to offer different IAS with different quality of service characteristics would be an example of this category.

Scope of Art. 3(3) (para. 78)

Art. 3(2) only allows contractual agreements related to technical conditions or technical characteristics of internet access that do not violate Art. 3(3). According to the draft guidelines, Art. 3(3) applies to practices "put in place by the ISP in the network when providing an IAS" (para. 78), but not to practices that are "endpoint-based" (paras. 78b, 32a&b). As the guidelines explain, this means that users are free to implement restrictions such as blocking or filtering in endpoints under their control – e.g., in terminal equipment in the sense of Art. 3(1) or in client application-based software (para. 78b). It also means that ISPs can potentially offer endpoint-based services that have the effect of blocking certain traffic, subject to Art. 3(2) (para. 78b, 32a&b).

It is important to note that clarification effectively narrows the protection provided by Art. 3(3) by introducing an additional criterion (that the blocking or filtering has to happen in the network) that is not present in the text of the regulation. This creates the danger that ISPs might use that limitation to circumvent the requirements of Art. 3(3) subparagraph 3 through the provision of end-point based services. Thus, the attempt to allow ISPs to reach competitive parity with third-party providers of endpoint based parental control and filtering services might inadvertently create a huge loophole. Given that Art. 3(3) (together with Art. 3(1)) is the heart of the regulation, such an outcome would be fundamentally incompatible with the regulation.

As a result, the distinction between (a) practices that happen "in the network" and therefore are subject to Art. 3(3) and (b) practices that are "endpoint-based" and, if offered by ISPs, are subject to Art. 3(2), is critical for distinguishing practices that violate the regulation from those that do not.

In drawing this distinction, the draft guidelines seem to follow the distinction between "devices in the network" and "end hosts" that is common in network engineering and one of the cornerstones of the internet's architecture.

I strongly support this approach. It allows the draft guidelines to draw on and be in line with concepts that are well-understood in the networking community. By limiting application-specific

functions such as blocking or filtering to higher layers at the end hosts and keeping them out of lower layers in the network, the regulation and the draft guidelines match the division of responsibility between the lower layers in the network and the higher layers at the end hosts that the Internet Engineering Task Force, network engineers and legal scholars view as critical for the Internet's architecture from a technical and policy perspective. In particular, this division of responsibility, which corresponds to the division of responsibility prescribed by the broad version of the end-to-end arguments, is critical for the Internet's ability to evolve, continue to support new applications, and foster innovation, free speech, and economic growth.

However, it seems that the draft guidelines in para. 78 provide an underinclusive description of what it means to for a practice to happen "in the network." The description also slightly deviates, likely inadvertently, from the way these concepts are normally used in networking. I recommend correcting this. The draft guidelines also do not provide an explanation of the terms "endpoints" and "endpoint-based services." Given the importance of these concepts for the application of the regulation to services like parental controls or filtering services, it seems useful to clarify these concepts.

At the highest level of a network architecture, designers distinguish two classes of components:[6] end hosts and computers in the core of the network. While end hosts are computers that use the network, computers in the core of the network form the network.

End hosts support users and run application programs; they use the services of the network to communicate with one another. The home computers many people use to surf the Internet, smartphones such as a the iPhone that allow users to use the Internet wherever they are, the Web servers that carry the content provided by Yahoo or the *New York Times*, or the servers through which users access their Gmail accounts are all examples of end hosts.

Computers in the core of the network form or implement the network.[7,8] They establish connectivity among the computers attached to the network. They include the cable modem termination system operated by a cable provider (to which a subscriber's cable modem is connected to give her access to the Internet), and the routers that network providers use to forward Internet data from one physical network to another. Viewed from computers in the core of the network, end hosts are the sources and destinations of data.

---

[6] van Schewick (2010a), pp. 50-52.

[7] This description glosses over the fact that in some network architectures, the end hosts may not only use, but also offer network services. In the Internet, the end hosts (or computers 'on' the network) also participate in the operation of the network through the protocols at the Internet layer and below. Thus, one may say that in the Internet, end hosts form the network, too. A more precise description of the Internet would focus on layers: the layers up to the Internet layer form or implement the network and are 'in' the network, while the layers above the Internet layer use the network and are 'on' the network. See, for example, Comer (2000), p. 186; Sterbenz and Touch (2001), p. 350.

[8] Throughout this comment, the term *the core of the network* will be used to denote the set of computers *in* the network, or, in the case of the Internet, the lower layers up to, and including, the Internet layer (see the preceeding note to this chapter). For a similar use, see Blumenthal and Clark (2001), pp. 71–72. Sometimes (but not in this comment), the term *core network* is used to denote the part of a hierarchical telecommunications network that provides the highest level of aggregation, such as the backbone network, as opposed to the intermediate part of the entire network, the backhaul that connects the core network with the access networks or edge networks.

Thus, the terms 'end hosts' and 'core of the network' denote a purely functional distinction between users and providers of communication services.[9] They do not refer to topological relationships or to administrative ownership and control. Thus, topologically, an end host may be co-located with routers belonging to the network's core. Similarly, a mail server is an end host regardless of whether it is owned and operated by an Internet access service provider.

Under the Internet's architecture, the division of responsibility between end hosts and devices that are in the network directly corresponds to a division of responsibility between higher and lower layers. While lower layers are implemented on end hosts and computers in the core of the network, higher layers only have to be implemented on end hosts.[10]

The last sentence in para. 78 directly maps to this distinction between the "end hosts" and "in the network:" "This means that the measures applied to the IP packet in the network of the ISP and before the IP packet has reached the destination IP address are considered to fall within the scope of Article 3(3)." (para. 78) This sentence is both accurate and sufficient to clarify the concept of "in the network."

The sentence before that, however, is underinclusive in two ways. I therefore recommend cutting it. Alternatively, the sentence could be moved to the end of the paragraph, with a "for example" to clarify that this is just one example of a practice to which Art. 3(3) applies.[11]

The sentence reads as follows: "BEREC considers that these rules apply when the processing of application layer protocol elements takes place before the IP packets have been received at the destination IP address provided by the end-user computer." (para. 78)

This sentence could be read to suggest that *only* measures that involve "*processing* of *application-layer* protocol elements" are subject to Art. 3(3). However, this sentence is underinclusive for two reasons and therefore does not provide an accurate encompassing definition of practices that are "in the network."

First, it is unclear what exactly "processing" entails. Does it only include measures that chage this information, or does it also include accessing information without changing it, for example if

[9] van Schewick (2010a), pp. 50-51, 378, 107-110.

[10] van Schewick (2010a), pp. 57-58. With respect to the International Standards Organization's Open Systems Interconnection reference model (the transport layer and higher layers are typically implemented on end hosts, not on the intermediate switches or routers), see, e.g., Peterson and Davie (2012), p. 32-33; Sterbenz and Touch (2001), pp. 41–42. With respect to the architecture of the Internet (end hosts implement all layers, while IP routers typically implement only lower layers, up to and including the Internet layer), see Kurose and Ross (2010), p. 54–55. In practice, routers may implement higher layers to terminate routing protocols such as BGP or management protocols.

[11] Suggestion: "78. Rules against blocking, slowing down, altering, restricting, interfering with, degrading or discriminating between traffic refer to measures put in place by the ISP in the network when providing an IAS. ~~*BEREC considers that these rules apply when the processing of application layer protocol elements takes place before the IP packets have been received at the destination IP address provided by the end-user computer.*~~ This means that the measures applied to the IP packet in the network of the ISP and before the IP packet has reached the destination IP address are considered to fall within the scope of Article 3(3). [Optional:] *For example, Art. 3(3) applies when the processing of application layer protocol elements takes place before the IP packets have been received at the destination IP address provided by the end-user computer.*"

a device drops a packet after it has accessed the URL that is part of the application-layer protocol element?

Second, the sentence suggests that only practices that process "application-layer" protocol elements are subject to Art. 3(3). (Thus, simply replacing "processing" with a broader term such as "accessing, interpreting or acting upon" would not solve the problem.) On the one hand, referencing only "application-layer protocol elements" links the concept of "in the network" to the layers of the Internet's architecture in a way that deviates from the way the concept is used in networking: In networking, layers up to the Internet layer are considered "in the network"; layers above the Internet layer (i.e. starting with the transport layer) are considered "on the network." Thus, both the transport layer *and* the application layer are layers that are "on the network." However, adding a reference to transport layer elements would still not capture all of the practices that are in the network and subject to Art. 3(3): After all, an ISP might block or discriminate against a packet based on the packet's sender or destination IP address. This kind of practice is clearly subject to Art. 3(3) and has to be captured by any definition of a practice that is "in the network." But in this case, the blocking does not involve "processing of any transport-layer or application-layer protocol elements" (i.e. of protocols in layers that are considered "on the network"), so it does not meet the definition provided in the sentence.

Thus, it seems preferable to focus on the fact that the practice happens "in the network of the ISP and before the IP packet has reached the destination IP address" (para. 78) rather than on the layer at which the practice is implemented or the layer which is accessed by the practice. This approach also best captures the wording of Art. 3(3) subparagraph 3, which focuses on the effect of the practice (i.e. "blocking" or "discrimination"), not on how the practice is implemented in the network.

Finally, it is worth noting that concluding that a certain practice is subject to Art. 3(3) does not mean it necessarily violates Art. 3(3). It only means that the practice will be evaluated under and needs to comply with Art. 3(3). For example, the existing version of the guidelines allows ISPs to use monitoring techniques as part of reasonable network management that access information contained in the transport layer header. While such monitoring is likely to happen "in the network of the ISP and before the IP packet has reached the destination IP address" (para. 78) and is thus subject to Art. 3(3), it is nevertheless allowed under Art. 3(3) second subparagraph and draft guidelines paras. 69 and 70.

The draft guidelines rightly clarify that the ISP's DNS resolver that is included with the IAS (the draft guidelines call this the "primary DNS resolver") is subject to Art. 3(3) as well (see para. 78a). This is consistent with the wording of Art. 3(3) which prohibits blocking regardless of how exactly is implemented. It ensures that ISPs cannot circumvent the protections in Art. 3(3) by implementing blocking via the DNS resolver that is provided by the ISP as part of the IAS. Any other interpretation would make the ban on blocking in Art. 3(3) meaningless. As Art. 1(1) makes clear, the goal of the regulation is to "safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services," and that requires the internet access service

sold by ISPs to be free of blocking or other discriminatory technical measures that violate Art. 3(3). Like all obligations imposed by Art. 3(3), this requirement is non-negotiable and cannot be waived as part of an agreement under Art. 3(2).[12]

End-point based restrictions (paras. 78b, 32a&b)

The draft guidelines clarify conditions under which ISPs can offer endpoint-based services that restrict access to certain destinations on the Internet, such as parental control or filtering software.

Third-party providers offer such end-point-based filtering services today. This includes, for example, third-party DNS services that allow users to customize content filtering for any devices that access a user's internet connection via the user's home network.[13] Clarifying the conditions under which ISPs can offer the same services would allow them to compete with these providers as long as they are not violating the provisions of the regulation.

However, the regulation establishes clear limits on the provision of such services, and the draft guidelines do not currently outline all of them. Clearly describing these limits is essential to avoid that the provision of endpoint-based filtering services becomes the loophole that makes the ban on blocking in Art. 3(3) meaningless.

Distinguishing endpoint-based filtering from filtering in the network prohibited by Art. 3(3)

First, Art. 3(3) of the regulation unequivocally prohibits ISPs from blocking or content filtering in the network. Filtering for parental control or content filtering in line with a user's wishes neither meets the requirements for reasonable traffic management under Art. 3(3) second subparagraph nor one of the exceptions the exceptions in Art. 3(3) third subparagraph (a)-(c). An exception related to parental controls and blocking unsolicited communications was deleted during the Trilogue negotiations, leaving no doubt about the legislative intent.

As explained above, this prohibition on blocking is non-negotiable and cannot be waived under Art. 3(2) as part of an ISP's agreement with an end user (see para. 37).

Allowing ISPs to sell an IAS that includes blocks certain websites, applications, or services would also violate the regulation's ban on sub-internet offers (see paras. 17, 38, 55).

While these points are clearly explained in the draft guidelines, the relevant discussion is spread throughout the guidelines. As a result, these points are not necessarily obvious to a reader of paras. 32a&b. Thus, it seems important to repeat these points at the beginning of para. 32a to provide much-needed context and to clearly highlight the distinction between the endpoint-based services discussed in 32a and the network-based filtering prohibited by Art. 3(3). Mentioning these points in para. 32a would also make clear that the discussion of endpoint-based filtering services is not meant to undermine or change the statements in paras. 78, 37, 17, 38, 55. Otherwise, an interested party could use the lack of such a clarification as an argument to

[12] However, ISPs can offer an *additional* DNS service that blocks access to certain websites as an endpoint-based filtering service under the conditions outlined below.
[13] See, e.g., https://www.opendns.com/home-internet-security/.

weaken these important protections when disputes about the interpretation of the guidelines arise.

Clarifying the concept of endpoint-based services

Under the revised version of the guidelines, Art. 3(3) leaves open the possibility of providing endpoint-based filtering services. Since these services are endpoint-based, the blocking or filtering doesn't happen "in the network" and is therefore not subject to Art. 3(3). They are, however, subject to Art. 3(2).

While these services are consistently described as endpoint-based in paras. 32a&b and 78b, it seems worth describing in more detail what constitutes an endpoint-based service. To the extent this is applicable, it might also be worth specifying that any ISP-provided endpoint-based services need to be directly addressed by the user and correctly terminate all layers of the protocol stack.

Clarifying the constraints imposed by Art. 3(2)

As set out above, the attempt to allow ISPs to offer endpoint-based parental control and filtering services in order to give competitive parity with third-party providers of such services by adding a new, unwritten criterion to Art. 3(3) creates the very real danger that this attempt inadvertently creates the loophole to the ban on blocking in Art. 3(3) that effectively makes the ban meaningless. Thus, BEREC needs to strike a delicate balance. In line with the regulation, the solution needs to maintain an unrestricted IAS as the default version, allow end users to freely decide whether they want the unrestricted default version of IAS or, if they want filtering, whether to use a third party filtering's software or their ISP's. It's one thing to give ISPs competitive parity and to give users who want a filtered internet an additional option to get it. It's another thing to do it in a way that undermines the regulation's decision for a neutral internet by making the default filtered, requiring users to expend effort to get the unfiltered version, or making the filtered IAS cheaper or higher quality than the unfiltered version. Finally, the attempt to give ISPs competitive parity should not result in allowing them to leverage their position as the user's ISP into a competitive advantage over third-party filtering services.

Art. 3(2) imposes constraints on agreements between ISPs and end users that are highly relevant to endpoint-based filtering services. In particular, Art. 3(2) prohibits such agreements from limiting end user rights under Art. 3(1) and from circumventing the provisions of the regulation under Art. 3(3) (see also Recital 7).

First, as discussed above, the regulation requires the IAS sold by ISPs to be free of blocking and filtering in the network or in the DNS included with the IAS (see paras. 78 and 78a). These requirements are non-negotiable and cannot be waived under Art. 3(2). As a result, an endpoint-based filtering service can only ever be offered *in addition to* the neutral IAS; it cannot replace aspects of that service. That means while an ISP might offer its customers the option of using a second, alternative DNS resolver that enables content-based filtering via the DNS, this can only be offered in addition to the "neutral" DNS resolver that is always included in and is the default option for the IAS. The endpoint-based service must be clearly marked as an additional service

and be opt-in and deactivated by default. Under the regulation, the default is a neutral IAS; users need to make an affirmative choice that they want to deviate from this. Similarly, users need to be able to revert back to the "neutral" default version of their IAS at any time. Thus, users need to have the ability to activate and deactivate the service.

Endpoint-based services may not be offered in a way that incentivizes users to use the restricted version of the IAS rather than the unfiltered IAS that the regulation intends to safeguard (see Art. 1(1)). That means, for example, that the decision to acquire or use the endpoint-based service cannot reduce the price of the IAS (which includes the "neutral" DNS) or improve the technical quality of the IAS, e.g. by offering higher speeds for the filtered version and lower speeds for the unfiltered version at the same price.[14] Allowing ISPs to effectively offer filtered IAS via endpoint-based service at a lower price or higher quality than "neutral" IAS would effectively re-create the regime that the regulation was designed to replace. Under the pre-2015 net neutrality regime, many ISPs offered cheaper plans that either contractually or technically prohibited the use of certain applications such as online telephony, while offering unrestricted plans at a higher price. Finally, allowing ISPs to incentivize users to choose the ISPs' filtered version of IAS over the unfiltered version would also distort competition between ISPs and third-party providers of endpoint-based services. Users have to affirmatively seek out endpoint-based services, and the use of endpoint-based services does not affect the price or quality of the IAS they are buying from their ISP. Using an ISP's endpoint-based service should not be different.

While these conditions seem to be implied by the draft guidelines,[15] they are so critical that they should be spelled out explicitly.

These requirements directly flow from the regulation; they are not optional. Endpoint-based services that do not meet these requirements violate the regulation. Thus, NRAS have to evaluate whether these services comply with these requirements and prohibit those that don't, and the guidelines should clarify this.[16]

Technical differentiation under the guidelines

With the revision of its guidelines, BEREC is the first regulator to formally consider how net neutrality protections should react to the upcoming rollout of 5G. This new generation of

[14] While the draft guidelines mention the potential impact of the use of such services on the price or quality of the IAS as one of the factors to consider in the evaluation of these services, they do not specify that the use of such services must not reduce the price or increase the quality of the neutral IAS.

[15] Nothing in the text of paras. 32a and b suggests that they are meant to override the requirement for the primary DNS resolver (i.e. the default DNS included with the IAS) in para. 78a, but this should be clarified. It is not clear whether the requirement that the IAS remains application-agnostic means that the IAS needs to continue to comply with Art. 3(3), and in particular, cannot block, filter, or discriminate in the network unless allowed by Art. 3(3).

[16] While the language in para. 23b "If either of these conditions are not met, an ISP should be deemed to be infringing the regulation" suggests that the factors in the bullet points are mandatory, the sentence introducing the bullet points ("the NRA may among other factors take into account the following") could be interpreted to mean that consideration of these factors is optional. While a summary sentence seems to be entitled to more weight in the interpretation, it is worth clarifying that complying with these factors is not optional.

wireless technologies promises speeds as high as 20Gbps with latency as low as one millisecond. Cell sites will also be able to handle many more devices connecting to them.

Simultaneously, 5G gives ISPs more ability to differentiate between apps and to wall off different parts of the network from others – sometimes referred to as network slicing.

In interactions with BEREC and elsewhere, European carriers have argued that the existing guidelines unduly limit their ability to use this new technology.

But whether and how to allow the use of differentiating technology is not really a new question. This kind of technology already exists; 5G just makes it easier for carriers to differentiate traffic, even as the explosion in capacity reduces the need to do so.

The existing guidelines establish a balanced framework that provides for "good" differentiation, while prohibiting "bad" differentiation. This framework allows ISPs to use the opportunities afforded by 5G to offer new and innovative services that do not violate net neutrality, while prohibiting them from using 5G technologies in ways that harm users, innovation, competition, and free speech. That's the way it should be.

Technical differentiation under Art. 3(2)

Under Art. 3(2), ISPs and customers of their IAS can contractually agree on technical conditions and technical characteristics of the service that do not violate Art. 3(3), as long as those agreements do not limit the exercise of the rights of end users under Art. 3(1). Art. 3(2) does not allow users to contractually waive an ISP's obligations under Art. 3(3) or Art. 3(1).

Within these constraints, the regulation gives ISPs the option to offer two new kinds of plans that are not explicitly allowed by the current version of the guidelines: (a) different plans that each provide a single type of service with quality of service characteristics that differ across plans and (b) plans offering user-paid, user-controlled quality of service that provide users the option of choosing different types of service within the same plan.

Differentiation between different internet access services under Art. 3(2) (paras. 34a&b)

It's long been clear that people's internet access needs differ. Dedicated gamers prioritize fast speeds. Independent content creators care about their upload speeds. Casual users care more about price than blazing speed, while businesses will pay a premium for guaranteed uptime.

Recognizing this, Art. 3(2) of the regulation allows ISPs to sell different kinds of internet access service at different prices to fit those needs. Recital 7 explicitly envisions the possibility that an ISP could sell different versions of internet access services with different speeds or data caps. As the existing version of the guidelines clarifies, such agreements do not violate Art. 3(3) and the rights of end users under Art. 3(1) when "data volume and speed characteristics are applied in an application-agnostic way" (i.e. without making distinctions among applications and classes of applications) (para. 34). That is, the speed of the service and the available data volume does not differ depending on which application or class of application a user uses.

By contrast, an IAS that consistently provided different speeds to different applications or different classes of applications (e.g., online telephony data packets receive speeds up to 1 Mbps, while data packets carrying online video receive speeds up to 1,5 Mbps) would violate the prohibition on discriminating among applications or classes of applications under Art. 3(3).[17] Thus, such a plan could not be contractually agreed on under Art. 3(2).

ISPs commonly sell IAS plans with different speeds and volume caps. When customers buy Internet access, they usually buy Internet access with a certain maximum speed (e.g., up to 20 Mbps) and, often, a certain data cap (e.g., 250 GB on a fixed network). A single Internet Service Provider might have different plans with different maximum speeds and different caps. Different customers might choose different plans, so different customers might have different maximum speeds and different maximum caps. But a particular customer's data packets will always receive the same type of service – a service called "best-effort service." All packets that a customer sends and receives get that service. In a network that offers "best-effort" service, the network does its best to deliver data packets, but does not provide any guarantees with respect to delay, bandwidth or losses. Thus, a best-effort service is very much like the default service offered by the postal service, which does not guarantee when a letter will arrive or whether it will arrive at all. Contrary to the postal service, where customers can choose services other than the default service like two-day shipping, the Internet access service offered to residential customers today provides only best-effort service.

In paras. 34a&b, the draft guidelines build on this model by clarifying that in addition to selling different IAS with different speeds and data volumes, ISPs might sell plans that have different Quality of Service characteristics such as latency (i.e. delay), jitter (i.e. variability of delay), or packet loss. For example, in addition to existing plans, an ISP might sell a premium plan that guarantees ultra-low delay and market it to avid gamers. The same provider could sell plans with guaranteed uptime Service Level Agreements, marketed to businesses. While the specific quality of service characteristics might differ among plans, all data packets transported under such a plan would still receive the same type of service with the characteristics of that plan. In other words, like the IAS plans already on the market, these new plans still offer the same type of service to each data packet transported under the plan; however, unlike existing plans, the single type of service offered by the plan might no longer be best-effort service, but have different quality of service characteristics, e.g., providing lower delay or a guaranteed bandwidth.

From a policy perspective, these plans are not a problem because all the data in a particular plan receives the same treatment. The plans do not pick and choose among applications, and a user can choose the plan that best fit their needs.

They are also clearly legal under the regulation. Since each data packet sent by a specific customer receives the same service with the quality of service characteristics associated with that

[17] While the regulation requires ISPs to manage their networks in ways that are as application-agnostic as possible, traffic management measures that temporarily differentiate among classes of applications might be justified under the conditions outlined in Art. 3(3).

customer's plan, the technical measures applied to the data packets to create a service with these characteristics do not discriminate between applications or categories of applications and therefore do not violate Art. 3(3) third subparagraph. Therefore, the agreement covering these characteristics is evaluated under Art. 3(2).

In particular, this means that the agreement must not limit the rights of end users under Art. 3(1) (Art. 3(2); see also para. 34a). This is a mandatory requirement that is established directly by Art. 3(2), and the text of para. 34a should reflect this. To bring the paragraph in line with the text of the regulation, the term "the practice *should* not limit the exercise of the rights of end users in laid down in Art. 3(1)" should be changed to "the practice *must not* limit ….".

Importantly, the regulation does not allow ISPs to limit the use of such a plan to specific applications or classes of applications. In other words, the single type of service offered by the plan needs to be offered and provided in an application-agnostic way (see para. 34a). Thus, an ISP can offer an IAS plan that provides lower delay then the normal best-effort service to all packets sent and received under the plan under Art. 3(2), but it cannot prohibit end users from using this plan for online telephony, nor can it technically limit the use of the plan to online games only. Such restrictions would violate the ban on blocking and discrimination among applications or classes of applications in Art. 3(3) third subparagraph and the regulation's ban on sub-internet offers in Art. 3(1), 3(2), and 3(3) (see paras. 17, 38, 55).[18] While this requirement is explicitly mentioned in para. 34a, it might be worth explaining in a bit more detail what it means. Since this requirement follows directly from Art. 3(3), compliance is mandatory. To reflect this, it might be advisable to change "NRAs *should* ensure that the implementation of different QoS levels is application-agnostic" in para. 34a to "To ensure compliance with Art. 3(3), NRAs *must* ensure …"

Like any other IAS, the provision of IAS under this kind of plan still needs to comply with Art. 3(3). This applies, for example, to measures designed to manage congestion under the plan. This requirement is not currently spelled out in the draft guidelines. To avoid any potential confusion, I recommend adding this requirement at the end of para. 34a.

Para. 34b rightly clarifies that premium plans with better quality of service characteristics may not "degrade[] the quality of other IAS subscriptions to a quality below the contract conditions agreed under Article 4(1)." This addresses an important problem. Para. 34b rightly explains the transparency obligations Art. 4(1) imposes on providers of such plans, and the tools that BEREC has available under Art. 4(1) and 5(1) to ensure an adequate level of quality for all plans.

Differentiation within an internet access service under Art. 3(2) (para. 34c)

Para. 34c also seems to allow a new kind of plan – plans that provide user-paid, user-controlled quality of service. While the plans discussed in the previous section provide the same type of service to all packets transported under a specific IAS plan, plans that provide user-paid, user-controlled quality of service offer users the option of using different types of service as part of a

[18] Of course, an ISP is still allowed to manage traffic under this plan in line with Art. 3(3).

single IAS plan. Thus, rather than receiving the same kind of service for everything they do online, internet service customers can choose different levels of service for specific activities.

Clarifying the treatment of such plans under the regulation is an important step. Plans that provide user-paid, user-controlled quality of service in line with the conditions outlined below are beneficial for users, allow ISPs to differentiate their services and charge for it, while avoiding the social costs associated with other kinds of quality of service. However, as currently written, the draft guidelines do not sufficiently specify the conditions under which such plans are allowed by the regulation. That's a problem, because in addition to violating the regulation, plans deviating from these conditions create the kinds of problems that net neutrality protections are designed to prevent.

Different applications have different requirements with respect to reliability, bandwidth or delay. For example, email can handle delay, but not missing packets, while online calls can handle missing packets, but are more delay-sensitive.[19]

So far, the lack of Quality of Service has not prevented real-time applications from becoming successful on the public Internet.[20] For example, although Internet telephony is sensitive to delay and high variations in delay ("jitter") and may benefit from a network service that provides low delay and low jitter, Internet telephony applications such as Skype or Vonage work well in the current Internet.[21] Video telephony applications like Skype or Google Video Chat function over today's broadband connections.[22] The same is true for online video and online games.

In other words, while some applications might benefit from special treatment that is more closely tailored to their needs, that does not mean that such special treatment is necessary for them to function on the normal Internet.[23] The guidelines rightly prohibit offering special treatment under the regulation's specialized services exception to applications that can function on the normal Internet, since such treatment is not necessary for these applications. This is critical for ensuring that the specialized service exception cannot be used to circumvent the regulation's ban on ISPs charging websites and apps for a fast lane to the ISPs' customers.

[19] For example, Internet telephony is very sensitive to delay above a certain level, but does not care about occasional packet loss. Users usually do not notice a one-way, mouth-to-ear delay of less than 150ms. A delay of more than 400ms makes voice calls frustrating or unintelligible. (International Telecommunication Union (2003); Kurose & Ross (2010), p. 601.) Depending on the encoding and loss-concealment mechanisms used, Internet telephony applications can tolerate between 1% and 20% of packet loss. (Kurose & Ross (2010), p. 617.) By contrast, e-mail is very sensitive to packet loss, but does not care about some delay. (See, e.g., Kurose & Ross (2010), pp. 92-94 and p. 95, Figure 2.4.) E-mail applications rely on a transport layer protocol called the Transmission Control Protocol (TCP) to get reliable data delivery. On the needs of applications more generally, see, e.g., Kurose & Ross (2010), pp. 92-95; Peterson & Davie (2012), pp. 530-37.

[20] Center for Media Justice, et al. (2010), p. 49-50; Open Internet Coalition (2010), pp. 33-35.

[21] Peterson & Davie (2012), p. 531.

[22] For example, Skype video requires a high-speed broad connection of at least 512kbps down / 128kbps up. For best quality, Skype recommends "a high-speed broadband connection of 4Mbps down / 512kbps up". Skype (2012).

[23] As a result, the guidelines rightly prohibit offering special treatment under the regulation's specialized services exception to applications that can function on the normal Internet

Still, while many applications function well with best-effort service, some applications may benefit from types of service that are more closely tailored to their needs. User-paid, user-controlled quality of service responds to this situation. It gives users the option to benefit from types of service other than best-effort service if and when they need it. Users, not their ISPs, freely decide which apps should get better treatment and when.

For example, in addition to the regular best-effort service that customers receive today, an Internet service provider could offer its Internet service customers the option of using an alternative level of service that provides a lower delay than the regular best-effort service. If a customer sends a data packet without specifying a particular service, that data packet will get the regular best-effort service customers get today (this service is often called the default baseline service). In addition, the customer has the option of choosing the low-delay service for specific data packets. One user might decide to use this low-delay service for certain online games; others might use it for online telephony or to upload a file before an important deadline.

To comply with the regulation, plans offering user-paid, user-controlled quality of service need to comply with the following requirements:

First, ISPs can make different types of service available as part of a single plan, but they cannot constrain how they can be used. Instead, the different types of service must be available equally to all applications and classes of applications.

This requirement makes it impossible for ISPs to use the provision of different levels of service as a tool to distort competition and interfere with user choice. It directly follows from Art. 3(3), third subparagraph. Limiting the use of a specific type of service to specific applications or classes of applications (e.g., making the low-delay service available only to the ISP's own video application or only to online games, but not to online telephony) would discriminate among applications or classes of applications, violating Art. 3(3) third subparagraph.

Second, the user is able to choose whether, when and for which application to use which class of service. As para. 34c rightly points out, this means "that end-users must have full control over which applications transmit traffic over which QoS level (e.g. by configuring the client application software) and that the QoS level in which specific applications are transmitted is not preselected by the ISP (e.g. based on commercial agreements with CAPs or the other end-user)."

This requirement puts users in control of their Internet experience and ensures that they can get the type of service they need when they need it. This requirement follows from Art. 3(3) third subparagraph as well. It ensures that the differential treatment associated with the actual provision of the different types of services in the network happens based on an application-agnostic criterion – the type of service chosen by the user for that particular packet. By contrast, providing different types of service to different applications or classes of applications chosen by the ISP would violate the ban on discrimination among applications and classes of applications in Art. 3(3) third subparagraph. The same is true when the ISP preselects the QoS level at which specific applications are transmitted. Practices that violate Art. 3(3) cannot be contractually

agreed upon under Art. 3(2) and the requirements in Art. 3(3) cannot be waived as part of a contract between the ISP and its customer.

Third, the ISP is allowed to charge only its own Internet service customers for the use of the different classes of service. It is not allowed to charge the end user, including providers of Internet applications, content, and service, at the other end of the connection.

If websites and applications can pay ISPs for faster access to the ISPs' customers, companies and speakers that cannot pay for such a fast lane will find it harder to compete and be heard. This hurts anyone who cannot afford to pay these fees: startups, small businesses, and speakers without deep pockets. This model also hurts smaller and rural ISPs, which do not have the market share to get paid by large companies for better levels of services, giving an unfair advantage to the larger ISPs they compete with.[24]

The prohibition on charging end users on the other side of the connection for the provision of the type of service stems directly from the regulation's ban on paid fast lanes.

An ISP's ability to charge its own end users for the provision of different types of service as part of a single plan follows from the fact that user-paid, user-controlled quality of service plans that meet the conditions outlined above do not violate Art. 3(3) and therefore can be offered under Art. 3(2) as part of an agreement on the technical conditions and characteristics of the service.[25]

By contrast, while the temporary provision of different types of service to different classes of applications might be justified under very narrow conditions under Art. 3(3) second subparagraph or the exceptions in Art. 3(3) third subparagraph (a)-(c), ISPs could not charge their customers an extra fee for the provision of different types of service as part of reasonable traffic management under Art. 3(3), since reasonable traffic management measures cannot be based on commercial considerations (see, e.g., Art. 3(3) second subparagraph).

Fourth, permitting ISPs to offer a plan that charges users for the use of better levels of service creates an inherent incentive for ISPs to degrade the regular level of service in order to encourage consumers to buy the better level of service for more of their Internet traffic. The existence of this incentive is well-documented in the economic literature on price discrimination. Most people are familiar with this problem from airlines, which have an incentive to make economy class uncomfortable enough so that people with money want to pay for business class. Economy class flights used to include several meals and have a reasonable amount of legroom; now fliers get a salty snack and the back of a seat in their face.

[24] For a longer analysis, see van Schewick (2015a), pp. 11-17. See also van Schewick (2010); van Schewick (2014b), Section "3. Allowing access fees is bad policy"; van Schewick (2014a), Section "Tough Lessons From Mobile and Music."

[25] As explained above, plans that do not meet the conditions outline above violate Art. 3(3) and therefore cannot be agreed on under Art. 3(2). For example, Art. 3(3) does not allow ISPs to continuously offer different types of service to different applications or classes of applications chosen by the provider. That would violate the ban on discrimination among applications or classes of applications in Art. 3(3) third subparagraph.

Today, delay-sensitive applications like online telephony, video-conferencing, video streaming or online gaming function perfectly fine the vast majority of the time over people's broadband Internet service. There is a danger that allowing ISPs to sell additional, better levels of service to their customers as part of a single IAS plan creates a situation where ISPs may be incentivized to degrade the level of regular service such that consumers will need to pay for a higher level of service to place the same online calls, participate in the same video conferences, play the same online games or watch the same videos.

The regulation gives national regulators the tools to address this problem. As para. 34b explains, "[a]ccording to 5(1), NRAs may also impose requirements concerning technical characteristics, minimum quality of service requirements and other appropriate and necessary measures to prevent degradation of the general quality of service of internet access services for end-users." This toolset also allows regulators to monitor the quality of the default baseline service offered by these plans (i.e. the service a packet receives if the customer does not select a different type of service) and prevent degradation of this service beyond an acceptable level.

Five, the provision of user-paid, user-controlled quality of service needs to be transparent to comply with Art. 4(1).

Six, like any IAS, the technical aspects of plans offering user-paid, user-controlled Quality of Service need to comply with Art. 3(3). In addition, like any agreement under Art. 3(2), such plans may not limit the rights of end users under Art. 3(1). This requirement, for example, might affect the way in which the different types of services can be priced.

User-paid, user-controlled Quality of Service that complies with the conditions outlined above offers the same potential social benefits as other, discriminatory or provider-controlled forms of Quality of Service without the social costs.

In particular, it preserves the application-agnosticism of the network, the principle of user choice, and the principle of innovation without permission:

First, this type of Quality of Service preserves the *application-agnosticism* of the network: The provision of Quality of Service is not dependent on which applications users are using, but on the Quality-of-Service-related choices that users make; thus, the network providers does not need to know anything about which applications are using its network in order for this scheme to work. Thus, contrary to plans in which ISPs decide which type of service to offer to which applications or classes of applications, this type of Quality of Service does not require the network provider to identify the different applications on its network in order to decide which class they belong to and determine the appropriate type of service – an activity that is complex, fraught with errors, and violates users' privacy. The ISP only makes different classes of service available, but does not have any role in deciding which application gets which Quality of Service; this choice is for users to make. As a result, ISPs cannot use the provision of Quality of Service as a mechanism to distort competition among applications or classes of applications.

Second, since users choose when and for which applications to use which type of service (in line with the principle of *user choice*), they can get exactly the Quality of Service that meets their preferences, even if these preferences differ across users or (for a single user) over time. For example, a consumer who is chatting with a friend might be happy to have Skype use the regular best-effort service. By contrast, a consumer who is doing a job interview over the Internet using Skype and does not want to be distracted by potential lags or hiccups in the call from network congestion might choose to use the low-delay service for her call, while continuing to use the regular Internet service for everything else. By contrast, ISPs often generally don't know the context from which a user's need for a specific type of service arises.

Third, in line with the principle of *innovation without permission*, an innovator does not need support from the network provider in order for his application to get the Quality of Service it needs. The only actors who need to be convinced that the application needs Quality of Service are the innovator, who needs to communicate this to the user, and the user, who wants to use the application. This greatly increases the chance that an application can get the type of service it needs. By contrast, technologies such as Deep Packet Inspection which ISPs use to identify apps to determine which type of service they should get are highly error prone and often misclassify apps. Misclassified apps do not get the type of service they need. Monitoring and fixing the problem requires a lot of work by ISPs and app makers. As with zero-rating schemes, only the largest ISPs and the largest apps can afford this; smaller apps will fall through the cracks.

Offering user-paid, user-controlled quality of service in line with the conditions outlined above is technically feasible. In fact, such plans are offered to business customers in the US today. For example, as part of its Private IP Network offering, Verizon Enterprise Services offers business customers the ability to mark their data packets with Differentiated Service Code Point (DSCP) markings. Verizon then provides each data packet the desired service as indicated by the marking, subject to the contractual agreement.[26] As part of its AT&T Business Fast Track offering (formerly known as AT&T Dynamic Traffic Management), AT&T offers business customers the option of using two premium services in addition to the regular baseline service on its mobile 4G/LTE network. Customers can request the desired service by marking data packets with DSCP markings.[27]

---

[26] See, e.g., http://www.verizonenterprise.com/external/service_guide/reg/cp_pip_plus_private_ip_service_2017MAY31_mk.pdf, p. 2 ("2.1.3.5 Class of Service Selection. Verizon will route Customer traffic based on the priority assigned by Customer using different classes of service designations, which follow the Internet Engineering Task Force Differentiated Services or Diff-Serv model. If Customer does not set different classes, Verizon will route all Customer traffic using the BE class as the default priority designation.")

[27] See, e.g., https://www.business.att.com/products/dynamic-traffic-management.html, Section "FAQs." (This offering does not fully comply with the conditions outlined above, since it contractually limits the availability of the premium classes to "qualified, business/mission critical applications." Premium classes cannot be used for "broadcasting video application and general consumer application such as Netflix, YouTube, or Facebook." (ibd.) Thus, it would fail the first condition outlined above and violate the prohibition on discriminating between applications and classes of applications in Art. 3(3) third subparagraph. However, the offering demonstrates the technical feasibility of such offerings.

Currently, it is not clear whether paras. 34a&b only apply to plans that each offer a single type of service with quality of service characteristics that differ among plans, or whether paras. 34a&b also apply to plans that offer user-paid, user-controlled quality of service. I think it is preferable to clearly distinguish between two cases, since both function differently, raise different policy concerns, and need to be evaluated in different ways. At the same time, both create a danger that ISPs might degrade the quality of a cheaper service to motivate customers to pay for a higher-quality service. In the first case, offering premium plans with more sophisticated quality of service characteristics might negatively affect the quality of more basic plans with lower quality of service characteristics – either as a consequence of the technical measures necessary to provide the quality of service characteristics of the premium plans or to motivate more affluent customers to subscribe to the more expensive premium plans. Thus, the degradation affects users of *other* internet access services. In the case of user-paid, user-controlled quality of service, an ISP might degrade the quality of the default baseline service offered as part of the plan in order to motivate customers *of that plan* to more often use the more expensive, higher quality service offered by the plan. Thus, the degradation affects the user's *own* internet access service.

A revised version of the guidelines could either clarify that paras. 34a and 34b apply to plans that each offer a single service, but with quality of service characteristics that differ among plans, and then use para. 34c to discuss the conditions under which user-paid, user-controlled quality of service is allowed under the regulation and lay out the necessary safeguards under Art. 4(1) and 5(1) to prevent a degradation of the default baseline service.

Alternatively, the guidelines could first discuss the characteristics of plans that each offer a single service, but with quality of service characteristics that differ among plans and the conditions under which these plans are allowed in para. 34a, followed by the corresponding discussion of user-paid, user-controlled quality of service in a new para. 34b. The problems related to a potential quality degradation in both cases could be discussed in a new para. 34c, which expands the current para. 34b to explicitly account for the degradation of the default baseline service in the case of user-paid, user-controlled quality of service.

Since it is not clear whether paras. 34a&b are meant to address user-paid, user-controlled quality of service as well, it is not clear which conditions are meant to apply to such plans. Assuming these plans are described solely in para. 34c, the paragraph mentions requirements (1) and (2), but not requirements (3)-(6). (In case paras. 34a&b are meant to apply to these plans as well, these paras touch on requirements (4)-(6), but do not mention requirement (3), either). Either way, to provide guidance to the market and ensure that potential plans offering user-paid, user-controlled quality of service are developed in compliance with the guidelines, it seems important to comprehensively list all of the conditions outlined above in one place. Given that these requirements follow directly from the text of the regulation and are mandatory, a revised para. 34c should frame them as such.

ISPs often complain that net neutrality protections in general and the BEREC guidelines in particular prevent them from offering new and innovative services and differentiating themselves

from their competitors. With the clarifications proposed above, the changes to paras. 34a-c would address these concerns without harming the values that the regulation is designed to protect. They give ISPs the option to offer two new kinds of plans that are not explicitly allowed by the current version of the guidelines: (a) different plans that each provide a single type of service with quality of service characteristics that differ across plans and (b) plans offering user-paid, user-controlled quality of service that provide users the option of choosing different types of service within the same plan. Thus, the changes would allow ISPs to offer new and innovative services, provide ample opportunity to differentiate themselves from their competitors, and earn money in the process.

Technical differentiation between internet access services and specialized services under Art. 3(5)

The regulation bans ISPs from offering technical preferential treatment (so-called "fast lanes") to providers of normal Internet applications, content, and services in exchange for a fee (Art. 3(3), subparagraph 2). There is a danger that ISPs could use the regulation's legitimate exception for specialized services to circumvent that ban. This is not a hypothetical threat. While the 2016 version of the guidelines mitigated this threat and BEREC is not proposing changes to the relevant parts of the guidelines, ISPs have continued to make clear that they want to use the specialized service exception to offer preferential treatment to everyday Internet application like online gaming, online telephony, video conferencing, or online video for a fee and are likely to continue to do so as part of this consultation.[28] In case this becomes relevant, I include by reference my comments on this topic in the 2016 consultation (attached).

Limits on the use of DPI (paras. 69&70)

Section 4 of BEREC's Public Consultation document for this consultation raises a series of questions regarding the existing limits on the use of Deep Packet Inspection in paras. 69 and 70 of the guidelines.

According to Art. 3(3) second subparagraph, reasonable traffic management measures "shall not monitor the specific content and shall not be maintained for longer than necessary." The current version of the guidelines clarifies that the transport layer payload constitutes "specific content," so measures monitoring the transport layer payload are prohibited (para. 69). By contrast, "traffic management measures that monitor aspects other than the specific content, i.e. the generic content, should be deemed to be allowed. … [I]nformation contained in the IP packet header, and transport layer protocol header (e.g. TCP) may be deemed to be generic content." (para. 70)

Although the draft guidelines under consultation do not propose any changes to these paragraphs, the Consultation Document suggests that BEREC is reconsidering the interpretation of the term "specific content." For example, the revised guidelines could limit the definition of "specific

[28] Deutsche Telekom (2015).

content" to the application layer payload, which would make it possible for ISPs to access the application layer header. Alternatively, the guidelines could exclude specific application-layer information from the definition of "specific content." In particular, the text of the consultation document suggests that domain names and URLs are being floated as information that ISPs would like to classify as "generic content."

The existing interpretation is required by the text of Art. 3(3) second subparagraph.

The regulation does not define the term "specific content." However, prohibiting ISPs from monitoring "specific content" suggests that there is a part of an IP data packet that ISPs are allowed to look at.

BEREC could have easily read the term "specific content" to refer to the entire payload of the IP data packet; that would mean the full transport layer packet would be off-limits. This interpretation would be in line with the way network engineers think about network protocols. Under the Internet's architecture, lower layers of the network (up to and including the Internet layer) should provide only general services of broad utility across applications in order to better support as many higher-layer applications as possible. The network should not be optimized to better support specific higher-layer applications. Instead, all application-specific functionality should be implemented in higher layers (transport layer and above) at the end hosts.[29] In line with this distinction, BEREC could have concluded that because all layers above the IP layer (i.e. transport layer and up) contain "application-specific" functionality, the full transport layer packet (i.e. the transport layer header and the payload) constitute content that is specific to applications and, therefore, specific content. Thus, the 2016 guidelines already classified parts of the IP data packet (i.e. the transport layer header) that network engineers view as "application-specific" as "generic content."

Broadening the interpretation of the term "specific content" to include the transport layer header in addition to the transport layer payload would mirror current developments in the evolution of Internet protocols. In October 2018, Sandvine estimated that about 75-90 percent of Internet traffic is already encrypted.[30] Most applications rely on Transport Layer Security (TLS) or its predecessor Secure Socket Layer (SSL). TLS encrypts the application-layer messages that are being exchanged over TCP. As a result, an ISP's deep packet inspection devices cannot "see" those application-layer messages.[31] While TLS effectively implements the current interpretation of the guidelines by encrypting the transport layer payload (i.e. the full application layer message), efforts are underway in the Internet Engineering Task Force to encrypt the transport layer header as well.

Even if BEREC does not want to follow this broader definition of "specific content," the regulation's protection for "specific content" makes clear that legislators felt that there is a part

[29] This design is a function of the broad version of the end-to-end arguments, which is considered to be one of the key architectural principles underlying the Internet by the IETF, network engineers, and policy scholars.
[30] https://www.sandvine.com/blog/global-internet-phenomena-encrypted-traffic-dominates-the-internet.
[31] Kurose & Ross (2013), pp. 711-717.

of a user's online communication that has to be protected from ISPs' spying eyes – that ISPs should not be able to discern the specifics of what a user is doing online. Such information is highly individualized and often sensitive.

Under this definition, the full transport layer payload (i.e. the full application layer message, which consists of the application layer header and the application layer payload) clearly constitutes "specific content."

This is obvious for the payload of the application layer. If a user requests a website using HTTP, the payload of the application layer message includes the actual website. If a user sends an email, the payload of the application layer message includes the text of the email. In an online call, the payload of the application layer message includes what the participants of the call say to each other. It cannot get more specific than that.

However, as para. 69 recognizes, the application layer header constitutes "specific content" as well. As the FCC determined in its broadband privacy rules in 2016, "the application header may reveal aspects of the application payload from which the content may be easily inferred—such as source and destination email addresses or website URLs."[32]

For example, the application layer header for email includes the email address of the sender and the receiver of the message, showing who is sending email to whom – providing a lot more information than that the person is sending an email. E-mail addresses included in the application layer header might even suggest something about the content of the actual email: For example, a person who is emailing a divorce lawyer might be considering or going through a divorce.

The application layer header for HTTP, the protocol that is used in web browsing, includes URLs. URLs, which provide the full path to the requested object, often give a pretty good indication of the content of the object. For example, the following three URLs from the Washington Post helpfully provide a summary of the actual content of the webpages: https://www.washingtonpost.com/politics/witness-testimony-and-records-raise-questions-about-account-of-trumps-no-quid-pro-quo-call/2019/11/27/425545c2-0d49-11ea-8397-a955cd542d00_story.html, https://www.washingtonpost.com/health/2019/11/27/birthrates-us-are-falling-abortions-have-also-hit-an-all-time-low/, https://www.washingtonpost.com/recipes/tamarind-and-honey-glazed-roast-turkey/17236/. That is not an accident: Keywords in full URLs are considered best practice by both websites and by search engines, which weight terms in the URL as a significant part of search rankings.[33] URLs provide information about specific health concerns that might be on a user's mind, whether it's http://www.scholarpedia.org/article/Amnesia or https://www.mayoclinic.org/diseases-conditions/hiv-aids/symptoms-causes/syc-20373524, and might even suggest a user's immigration status such as https://www.loveisrespect.org/legal-help/help-for-undocumented-immigrants/, a website that providers legal advice for undocumented immigrants in an abusive

[32] https://www.fcc.gov/document/fcc-releases-rules-protect-broadband-consumer-privacy, p 41.
[33] https://moz.com/learn/seo/url.

relationship. URLs may also include information that is an integral part of the interaction a user has with the site. For example, as Steve Bellovin has explained,

> "For example, the path can include a "query" subcomponent. This is a special part of a URL path preceded by a "?" that supplies additional information to the web server about the service being requested. In some cases, this reflects information entered by the user, such as a search query, for example:
>
> **https://www.google.com/search?q=what+is+metadata**
>
> Here, we have the URL generated by entering "what is metadata" into the Google search box. The "?q=what+is+metadata" query sub-component reflects the text entered by the user."[34]

Search queries provide highly personal information, a direct window into a user's mind.

Thus, in all of these cases, information contained in the application header provides information about the specifics of what a user is doing online, rather than just providing an indication of the type of activity a user is engaged, making the classification of the application layer header as "specific content" a natural fit.

As the examples show, application headers can convey highly sensitive information which receives particular protection under European privacy law, so the clear goal of the provision (i.e. to protect user's interest in protecting their privacy) strongly favors this conclusion as well. The GDPR explictly bans "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" without affirmative user consent.[35]

As the discussion shows, trying to establish a limited exception from the definition of "specific content" for URLs would fail for the same reasons.

This leaves domain names. The Domain Name System (DNS) translates human-readable names into IP addresses. At first sight, this might suggest that they are no different from IP addresses, which the guidelines already classify as "generic content." This conclusion, however, is not correct. While certain IP addresses correspond to and might be traced back to a single provider, a single IP address can host many different web servers with different domain names. More importantly, like URLs, domain names can expose information that is highly suggestive of the specific activity the user is engaging in and can reveal highly sensitive information.

For example, the domain name womenonwaves.org is the web address of an organization that provides abortion information to women in countries where abortion is illegal and which runs campaigns where it provides abortions to women in such countries via a ship parked in

[34] https://jolt.law harvard.edu/assets/articlePDFs/v30/30HarvJLTech1.pdf, p. 66.
[35] https://gdpr-info.eu/art-9-gdpr/, Article 9 paragraph 1.

international waters just offshore from those countries. This is just one example. The specific activity a user engages in might be as obvious as buycialis.com or RedTube.com (a pornographic content). Visiting a medical site like Mayo.com indicates an interest or concern in health issues (rather than just the fact that the user is surfing the web) or even a specific health problem (e.g., visiting aa.org, the website of Alcoholics Anonymous). Whether someone visits nytimes.com (the domain of the New York Times), wsj.com (Wall Street Journal), or breitbart.com can indicate a person's political leanings. It can also be less obvious: for example, popular streaming video sites such as Crunchyroll, Fanimation, Spuul.com or UMC.TV can reveal personal interests or your likely ethnicity.

For this reason, the Internet Engineering Task Force has long viewed the domain names visited by a user as deeply private information, whose exposure presents significant privacy risks and which should therefore be kept private.[36] Thus, as the U.S. Third Circuit Court of Appeals found, "routing information and content are not mutually exclusive categories."[37]

Thus, under both criteria outlined above (does part of the data packet under consideration provide information contained in the application header provide information about the specifics of what a user is doing online, rather than just providing an indication of the type of activity a user is engaged or does it potentially reveal highly private and sensitive information), domain names constitute "specific content."

Importantly, the concerns about ISP access to and monitoring of the information discussed so far do not change depending on whether this access happens in the context of traffic management or zero-rating. They are just as salient for zero-rating products. In fact, accessing this information in the context of determining whether a user accesses content that is part of a zero-rating program can make it more likely that domain names or URLs reveal sensitive information about a user. For example, many zero-rating programs zero-rate online video. Video entertains and informs, so someone's video preferences reveal a lot of very private information about that person. Even without having access to the specific URL accessed by a user, seeing the domain might be sufficient. For example, as the number of providers included in open zero-rating programs increases, sites such as NRA.TV (the video offerings of the National Rifle Association) or the The Young Turks (TYT.com), a progressive news and opinion program could join. Any end-user visiting those sites would have their traffic identified and expose sensitive political information about themselves to their ISP. Other revealing information beyond politics can be similarly exposed through domain names alone. For example, PornTube.com (there's no legal reason this kind of site can't join a zero-rating program), Men.com (an adult video site for gay men) or UMC.TV (Entertainment by and for the Black community) could also be a part of a video-streaming category-focused zero-rating scheme. Again, the domain name alone allows conclusions about the most private of information such as sexual orientation or racial or ethnic origin, which receives particular protection under the GDPR.

[36] The Internet Engineering Task Force's (IETF) RFC 7626, "DNS Privacy Considerations" is widely viewed as the canonical technical statement of the associated privacy issues. https://tools.ietf.org/html/rfc7626.
[37] https://scholar.google.com/scholar_case?case=11228916892177508504.

Thus, the text of Art. 3(3) subparagraph 2 and the goal of the provision strongly support either broadening the definition of "specific content" or keeping the current definition intact.

Other consideration point in the same direction.

There is no need to change the interpretation in order to allow ISPs to engage in traffic management. In fact, allowing ISPs to use DPI to look at information beyond the transport layer header may harm users and app providers.

ISPs argue they need to be able to monitor the application layer header or, at least, URLs and domain names to identify applications so that they can differentiate among different classes of applications.

First, the guidelines make clear that class-based traffic management can only be used as a last resort if application-agnostic traffic management cannot solve congestion. (This point is explained in detail in the section of my 2016 comments on traffic management, which I attach and hereby include by reference.) In the US, fixed ISPs have managed congestion in application-agnostic ways, so class-based congestion management will generally not be necessary on fixed networks. With the increase in capacity associated with the move to 4G and 5G, the need for congestion management that distinguishes among classes of applications is likely to decrease significantly.

Second, the information available to ISPs under the current interpretation of "specific content" is helpful in identifying applications and types of applications. ISPs are allowed to access the IP addresses of the source and destination of the traffic, which in certain cases directly maps to a specific application or content provider. As part of the transport layer header, ISPs can identify the transport layer protocol and can "see" the port numbers at the source and destination, which may allow the ISP to make inferences about the protocol that is using TLS (e.g., HTTPS often uses port 443).[38] Thus, an ISP may be able to infer from the port numbers that the application is using HTTPS, which is helpful, but it cannot see the content of the messages transferred by HTTP, so it doesn't know whether the application is using HTTP to transfer text, audio, or video.

Third, the current interpretation of "specific content" does not prevent ISPs from "'*responding* to' the QoS requirements of categories of traffic in order to optimize the overall transmission quality and enhance the user experience" (para. 64) as envisioned by Art. 3(3) second subparagraph and Recital 9. As para. 64 rightly points out, ISPs can "rel[y] on the information provided by the application when packets are sent into the network" "in order to identify categories of traffic" for differential treatment under Art. 3(3) second subparagraph, should the conditions for this kind of class-based traffic management be met. This kind of information is part of the IP packet header and does not require access to those parts of the packet that are off-limits under the existing definition of "specific content."

As explained in the section on user-paid, user-controlled quality of service, this is not a hypothetical option. Several providers in the US already offer plans that allow business customers of mobile and fixed internet access to mark their data packets with the desired type of

[38] GSM Association (2015), pp. 21-22.

service using Differentiated Services Code Point (DSCP) markings in the IP packet header, which is then honored by the ISP. Thus, signaling an application's quality requirements is technically feasible.

Fourth, relying on information provided by the application as part of the IP packet header is not only feasible, but is preferable to accessing parts of the transport layer payload to identify applications.

There's no technology that can identify and classify apps automatically. DPI constantly misclassifies apps,[39] and since the most internet traffic uses HTTPS or other forms of encryption by default, routers can't look deeply into a packet to determine what it is. Remaining workarounds like DNS-snooping are closing.

That means many apps would not get the service they need and could even be put into buckets that harm them. We saw this in the UK, when games often stopped working in the evening, because ISPs were identifying them as peer-to-peer file-sharing applications, which the ISPs were throttling. This harms users, whose applications do not get the service they need, and app providers whose apps do not function as well as they should.

The inevitable misclassifications require lots of work by both carriers and app makers to monitor and fix these problems. As with zero-rating schemes, only the largest ISPs and the largest apps can afford this; smaller apps will fall through the cracks.[40]

These kinds of considerations (i.e. harm to innovation and user rights) are highly relevant when interpreting a regulation that explicitly aims to preserve the internet as an engine of innovation and protect end users' rights to use the applications and services of their choice (Art. 1(1), Art. 3(1) and Recital 1).

Similarly, the use of URLs or domain names is highly susceptible to fraud. As Sandvine and other have documented, malicious users or app providers can easily trick the zero-rating program into misclassifying an app that is not part of the zero-rating program as one that is by putting the URL or domain name of a zero-rated app into the relevant part of the data packet.[41]

Finally, reducing the level of protection for the information users are forced to expose to their ISP in the course of using their internet connection by narrowing the definition of "specific content" runs counter to a number of trends towards more, not less, protection for user's information.

Following the revelations about widespread surveillance on public communications networks, the Internet Engineering Task Force has been engaged in an aggressive effort to encrypt all

[39] For an in-depth study of the problems with misclassification of DPI in the context of traffic management in the UK, see Cooper & Brown (2015). See also Yiakoumis, Katti & McKeown (2016), pp. 3-4.
[40] For a detailed description, see Cooper & Brown (2015), pp. 13-15.
[41] For a general, in-depth discussion, see https://www.sandvine.com/download-the-whitepaper-zero-rated-fraud-prevention. For a study of T-Mobile's Binge On program coming to the same conclusions, see https://david.choffnes.com/pubs/bingeon_sigcomm16.pdf, pp. 5-6.

layers of the internet protocol stack.[42] Large players like Google, Facebook, and Netflix and the offering of HTTPS as a service by cloud providers and Content Delivery Networks have helped drive the deployment of encryption.

These efforts have been widely successful. In October 2018, Sandvine estimated that about 75-90 percent of Internet traffic is already encrypted.[43] Most applications rely on Transport Layer Security (TLS) or its predecessor Secure Socket Layer (SSL). TLS encrypts the application-layer messages that are being exchanged over TCP. As a result, an ISP's deep packet inspection devices cannot "see" those application-layer messages.[44] Thus, TLS effectively implements the current interpretation of the guidelines by encrypting the transport layer payload (i.e. the full application layer message).

Even with encryption, ISPs can often access information about the domain name by intercepting the user's communication with the DNS, which is generally not encrypted. Alternatively, if the packet is encrypted using TLS, an ISP can access the Server Name Identification (SNI) field, which transmits the name of the server that the user is trying to access. In this case, the ISP is able to observe the name of the server (e.g., https://cyberlaw.stanford.edu) that the client is trying to contact as part of the connection set up, but not the full path of the content that is being transferred (e.g., https://cyberlaw.stanford.edu/blog).

However, both of these workarounds are closing. The secure version of DNS standardized by the IETF, DNSSec, which encrypts the domain name, is currently being deployed. Both Mozilla and Google have recently launched DoH, or DNS over HTTPS, specifically as a way to provide user privacy by encrypting DNS queries so that requested domain names are not visible to ISPs.[45] The IETF works actively on encrypting the SNI field; and large players like Cloudflare are already encrypting SNI.

Thus, even if BEREC changed the interpretation of "specific content" and allowed ISPs to access the application layer header in general or domain names and URLs specifically, the practical impact of this legal change on ISPs' ability to manage their networks would be small and rapidly diminish further.

The IETF recognizes that successively making more and more parts of an IP data packet inaccessible to ISPs via encryption might interfere with methods ISPs have traditionally used to manage traffic[46] and is working actively to help foster the development of alternative traffic management methods that function in the presence of widespread encryption.[47] However, the IETF has decided that protecting users' privacy is more important than preserving existing approaches to traffic management, providing a good role model for BEREC.

---

[42] See https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/, https://tools.ietf.org/html/rfc7624, and https://tools.ietf.org/html/rfc7258.
[43] https://www.sandvine.com/blog/global-internet-phenomena-encrypted-traffic-dominates-the-internet.
[44] Kurose & Ross (2013), pp. 711-717.
[45] https://support mozilla.org/en-US/kb/firefox-dns-over-https and https://blog.chromium.org/2019/09/experimenting-with-same-provider-dns.html.
[46] See, e.g., https://tools.ietf.org/html/rfc8404 and https://tools.ietf.org/html/rfc8517.
[47] See, e.g., https://datatracker.ietf.org/doc/draft-smith-encrypted-traffic-management/.

In sum, narrowing the definition of "specific content" would encourage ISPs to rely on an anachronistic technology that creates problems and violates users' privacy. By contrast, maintaining the existing interpretation would provide an additional incentive for ISPs to contribute to the refinement of next-gen traffic management practices that respect users' privacy while allowing ISPs to manage their networks.

Zero-rating and other forms of differential pricing

The regulation's framework for evaluating zero-rating

Observers often comment that the regulation provides little guidance to regulators when evaluating zero-rating plans. By contrast, the regulation establishes a framework for evaluating zero-rating and other forms of differential pricing that is much more nuanced than often assumed. While the guidelines are consistent with this framework, they do not explicitly set it out. Thus, it might be helpful to start by laying out this framework.

Zero-rating is a commercial practice under Art. 3(2) of the regulation. That Article says that commercial practices should not limit the right of end users under Art. 3(1).

According to Recital 7, regulators "should be empowered to intervene against agreements or commercial practices which, by reason of their scale, lead to situations where end-users' choice is materially reduced in practice." Regulators "should be required … to intervene when agreements or commercial practices would result in the undermining of the essence of the end-users' rights."

Some observers (but not the guidelines) view the term "limit" in Art. 3(2) as synonymous with "material reduction of end users' choice," assuming that Recital 7 establishes a ceiling for regulatory intervention. Under this view, if a commercial practice reduces the rights of end users without "materially reducing users' choice in practice," regulation does not provide a possibility for regulatory intervention.

I suspect this interpretation is based on a misunderstanding of the structure of Art. 3(2). In fact, regulators' ability to enforce Art. 3(2) is much broader.

First, Art. 3(2) allows regulators to intervene if a commercial practice limits the rights of end users under Art. 3(1).

Second, Art. 5(1) gives regulators the power to enforce Articles 3 and 4. That means regulators can intervene based on this Article when zero-rating or another agreement or commercial practice limits the exercise of these rights.

Third, Recital 7 establishes some minimal requirements for when regulators should act. Regulators can always act to enforce the rules under Art. 5(1), but at a minimum, they *should be empowered to* intervene if there is a material reduction in users' rights. And they are *required* to

intervene when zero-rating undermines the essence of these rights. Thus, Recital 7 provides a floor, not a ceiling for what NRAs can do with respect to zero-rating or other commercial practices. It does not limit NRAs' ability to enforce the rules to cases where there is a material reduction or the zero-rating undermines the essence of this right. Any other interpretation would not adequately reflect the role of recitals in EU law. Recitals can clarify or help interpret an article in a regulation, but they cannot independently create or remove obligations. Thus, Recital 7 cannot take away the power to enforce Art. 3(2) that another article of the regulation (Art. 5(1)) confers on regulators. Para. 45 of the guidelines reflects that insight.

(As the text and structure of Recital 7 makes clear, the instruction in Recital 7 to consider the market positions of ISPs and CAPs is only relevant for the question whether there is a material reduction, but not for the question whether the zero-rating undermines the essence of user rights.)

Fourth, like all ISP practices, zero-rating has to comply with the rules regarding traffic management under Art. 3(3). Thus, as the guidelines recognize correctly in paragraph 38, zero-rating offers that block or slow down only applications that are not zero-rated when a user hits her monthly cap, while not applying the same measures to zero-rated application would violate Art. 3(3).

In sum, Art. 3(2) and Recital 7 create the following framework for regulatory intervention:

- if a commercial practice reduces the rights of end users without "materially reduc[ing] end-users' choice in practice," regulators can intervene based on Art. 3(2) and Art. 5(1);
- if a commercial practice "lead[s] to situations where end-users' choice is materially reduced in practice," regulators should be required to intervene; and
- if a commercial practice "undermin[es] the essence of the right" in Art. 3(1), regulators are required to intervene;
- if a commercial practice includes technical measures, these measures are evaluated separately under Art. 3(3).

BEREC has the power to ban certain harmful forms of zero-rating in the guidelines

The framework described above gives BEREC the power to enact bright-line rules banning certain harmful forms of zero-rating outright. To do so, it needs to specify in the guidelines that the practice in question "undermines the essence of the right" in Art. 3(1). Because of Recital 7, regulators are then required to intervene and enforce the regulation.

In evaluating zero-rating under Art. 3(2), regulators can consider the following aspects:
According to Art. 3(1), commercial practices should not limit the right of end users under Art. 3(1) to access the applications, content, and services of their choice, and to distribute and provide the applications, content, and services of their choice. Thus, the regulation protects the rights of end users as *consumers* and *producers*. That means that regulators can consider the impact of zero-rating on both consumers and application and content providers.

Moreover, Art. 3(2) must be interpreted in light of the goals of the regulation to protect the rights of end users and ensure the continued functioning of the Internet ecosystem as an engine of innovation.

Finally, according to Recital 33, "[t]he Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter [of Fundamental Rights of the European Union], notably the protection of personal data, the freedom of expression and information, the freedom to conduct a business, non-discrimination and consumer protection." The Charter of Fundamental Rights of the European Union binds European institutions and national authorities when they implement and apply European Union law, including when they are applying a regulation.[48] As a result, regulators need to interpret the provisions of the regulation and the corresponding recitals in a way that respects these fundamental freedoms. Thus, the impact of ISP practices on freedom of expression and information, which includes the freedom not just to receive, but also to seek and impart information, and on media pluralism, are highly relevant to regulators' analysis.[49]

Thus, the regulation protects end users not only in their roles as consumers and producers in the economy, but also as speakers and listeners in our democracy.

The draft guidelines appendix with a step-by-step approach to zero-rating should be deleted.

The draft guidelines add a new appendix to evaluate zero-rating. However, the appendix misses many of the important clarifications on how to evaluate zero-rating included in the text of the guidelines. For example, they do not include the important language regarding the discussion explaining that plans that only zero-rate a few apps in a class or plans that are closed are more likely to constitute a material reduction or undermine the essence of user rights. They do not include the reference to content diversity and speech. They also miss some of the bullet points in para. 48.

The best approach seems to delete the appendix. Alternatively, BEREC could clarify that the appendix is not meant to supersede or replace the more detailed discussion in the actual text of the guidelines.

Attachments

van Schewick, Barbara. 2015. The Case for Meaningful Network Neutrality Rules. Report submitted as Attachment to Barbara van Schewick's Ex Parte in the Matter of Protecting and Promoting the Open Internet submitted February 20, 2015 to the Federal Communications Commission GN Dkt. No. 14-28.
Report: http://apps.fcc.gov/ecfs/document/view?id=60001031682

[48] See Art. 51(1) of the Charter. See also http://ec.europa.eu/justice/fundamental-rights/charter/index_en htm.
[49] See Art. 11(2) "Freedom of Expression and Information" of the Charter, which states: "The freedom and pluralism of the media shall be respected."

All documents filed with FCC, including cover letter, report and attachments to report: http://apps.fcc.gov/ecfs/comment/view?id=60001018648

van Schewick, Barbara. 2015. "Network Neutrality and Quality of Service: What a Nondiscrimination Rule Should Look Like." Stanford Law Review, 67(1): 1-166. Article: http://www.stanfordlawreview.org/sites/default/files/67_Stan_L_Rev_1_van_Schewick.pdf

van Schewick, Barbara 2016. Comments in BEREC net neutrality consultation.

Cooper, Alissa & Ian Brown. 2015. "Net Neutrality: Discrimination, Competition, and Innovation in the UK and US." ACM Transactions on Internet Technology, 15(1): Article 2.

Yiakoumis, Yiannis, Sachin Katti & Nick McKeown. 2016. "Neutral Net Neutrality." Paper to be presented at ACM SIGCOMM 2016. Florianópolis, Brazil. http://yuba.stanford.edu/~yiannis/neutral-net-neutrality.pdf

References

Center for Media Justice, Consumers Union, Media Access Project, New America Foundation & Public Knowledge. 2010. Comments of Public Interest Commenters to Federal Communications Commission. GN Docket No. 09-191. January 14. http://apps.fcc.gov/ecfs/document/view?id=7020378818

Cooper, Alissa & Ian Brown. 2015. "Net Neutrality: Discrimination, Competition, and Innovation in the UK and US." *ACM Transactions on Internet Technology*, 15(1): Article 2.

Deutsche Telekom. 2015. "Net neutrality: Finding consensus in the minefield." October 28. https://www.telekom.com/media/management_unplugged/291728

Federal Communications Commission. 2014. "Open Internet Roundtable - Policy Approaches." September 16. https://www.fcc.gov/news-events/events/2014/09/open-internet-roundtable-policy-approaches

Frischmann, Brett M. & Barbara van Schewick. 2007. "Network Neutrality and the Economics of an Information Superhighway: A Reply to Professor Yoo." *Jurimetrics Journal*, 47(4): 383–428.

GSM Association. 2015. *Network Management of Encrypted Traffic. Version 1.0.* GSM Association. http://www.gsma.com/newsroom/wp-content/uploads/WWG-04-v1-0.pdf

International Telecommunication Union. 2003. *ITU-T Recommendation G.114: One-way transmission time.* International Telecommunication Union. G.114. http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.114-200305-I!!PDF-E&type=items

Kroes, Neelie. 2012. "Next Steps on Net Neutrality – Making Sure you get Champagne Service if That's What You're Paying For." *European Commission.* May 29. http://blogs.ec.europa.eu/neelie-kroes/netneutrality/

Kurose, James F. & Keith W. Ross. 2010. *Computer Networking: A Top-Down Approach.* 5th ed. Boston, MA: Pearson/Addison Wesley.

Kurose, James F. & Keith W. Ross. 2013. *Computer Networking: A Top-Down Approach.* 6th ed.: Pearson.

Open Internet Coalition. 2010. Comments to Federal Communications Commission. GN Dkt. No. 09-191. January 14. http://apps.fcc.gov/ecfs/document/view?id=7020377928

Peterson, Larry L. & Bruce S. Davie. 2012. *Computer Networks: A Systems Approach.* 5th ed. Burlington, MA: Morgan Kaufmann.

Skype. 2012. "Get Skype for Windows." February 21. http://www.skype.com/intl/en-us/get-skype/on-your-computer/windows/

van Schewick, Barbara. 2007. "Towards an Economic Framework for Network Neutrality Regulation." *Journal on Telecommunications and High Technology Law*, 5(2): 329-391.

van Schewick, Barbara. 2010. *Opening Statement at the Federal Communications Commission's Workshop on Approaches to Preserving the Open Internet.* Federal Communications Commission. http://www.law.stanford.edu/display/images/dynamic/publications_pdf/schewick-statement-20100428.pdf

van Schewick, Barbara. 2014a. "The Case for Rebooting the Network-Neutrality Debate." *The Atlantic.* May 6. http://www.theatlantic.com/technology/archive/2014/05/the-case-for-rebooting-the-network-neutrality-debate/361809/

van Schewick, Barbara. 2014b. "The FCC Changed Course on Network Neutrality. Here is Why You Should Care." *Stanford Center for Internet and Society Blog.* April 25. http://cyberlaw.stanford.edu/blog/2014/04/fcc-changed-course-network-neutrality-here-why-you-should-care

van Schewick, Barbara. 2015a. *The Case for Meaningful Network Neutrality Rules.* Attachment to Barbara van Schewick's Ex Parte in the Matter of Protecting and Promoting the Open Internet submitted February 20, 2015 to the Federal Communications Commission GN Dkt. No. 14-28. http://apps.fcc.gov/ecfs/document/view?id=60001031682

van Schewick, Barbara. 2015b. "Network Neutrality and Quality of Service: What a Nondiscrimination Rule Should Look Like." *Stanford Law Review*, 67(1): 1-166.

Yiakoumis, Yiannis, Sachin Katti & Nick McKeown. 2016. "Neutral Net Neutrality." Paper presented at SigComm 2016. Florianópolis, Brazil.