European Net Neutrality at the beginning of a new era

European net neutrality is at the beginning of a new era. Through the net neutrality Regulation adopted in 2015[1], and corresponding net neutrality Guidelines issued in 2016[2], a new foundation for protection of the open Internet in Europe is established. The regulatory monitoring of net neutrality at the national level, as prescribed by the Regulation, should be the guarantee for a neutral Internet for European citizens and businesses.

By Frode Sørensen, Senior Advisor, Norwegian Communications Authority (Nkom)

The goal of net neutrality is to protect the value of the Internet for end-users, for the industry, and for the overall democratic society. In concrete terms, net neutrality boils down to equal treatment of traffic on the Internet, whereby end-users themselves can decide how to use their own Internet access, and whereby entry barriers for content and application providers (CAPs) are low. As a result of non-discriminatory treatment, the Internet should remain an open platform for communication useable for any purpose, stimulating the flourishing of social, democratic, cultural, and economic development.[3]

The fundamental characteristic of such an open platform is that it becomes application-agnostic, where applications running on end-user equipment receive equal treatment of traffic transmitted over the Internet. This architecture is also referred to as the end-to-end principle[4], where application can run in endpoints connected to the Internet, without specific adaption inside the network. The application layer is decoupled from the underlying network layer, facilitating "innovation without permission", whereby a large number of innovators face low barriers when developing and deploying their applications.

This paper explores the background and emergence of the European net neutrality Regulation (section 1), as well as the rules of the Regulation. Regarding the latter, the focus will be on three core issues that have attracted policymakers' and regulators' attention over the past year: zero-rating and other commercial practices (section 2); the distinction of different levels of traffic management (section 3); and the so-called specialised services (section 4). Finally, some concluding remarks are given (section 5).

The goal of the paper is to illustrate how the European net neutrality Regulation facilitates flexible network technology innovation, at the same time as it safeguards innovation at the edge of the network. The Regulation therefore constitutes a futureproof framework for regulatory supervision and enforcement of net neutrality which maintains continued evolution of the Internet architecture and ecosystem.

[1] Regulation 2015/2120

[2] BEREC (2016a)

[3] See e.g. van Schewick (2010)

[4] IETF (1996)

1. Evolution of European net neutrality

Looking back at the timeline of net neutrality in Europe, it has been a journey over several years. Using the 2009 Regulatory Framework[5] as a reference, it consists of a seven years' history with ups and downs. This framework had its good intentions, but was over time judged by the political institutions as insufficient to protect net neutrality.

It has been argued that access regulation in Europe should be sufficient to ensure net neutrality, since end-users could switch to alternative Internet service providers (ISPs) to achieve neutral Internet access.[6] However, an essential characteristic of Internet communication is ignored in this argument; as an Internet user you are depending on the users in the other end which you communicate with. Many of those will not switch to a neutral access due to the pricing policy of their ISPs. Thereby the Internet becomes fragmented, and the network effect is significantly reduced.

In this period, BEREC on request from the European Commission conducted a traffic management investigation[7] among European operators. The results from this investigation showed that on average, every fifth European subscriber to fixed Internet access, and as much as every third subscriber to mobile Internet access experienced restrictions to the use of their own Internet access service, such as blocking of VoIP.

Over the last years, different national approached to net neutrality evolved. Norway has the longest running net neutrality regime in Europe. Based on a co-regulatory approach, not to be confused with a self-regulatory approach, national net neutrality guidelines were established in Norway in 2009[8]. These guidelines contained rules against blocking and throttling of applications, essential to achieve net neutrality.

The Netherlands and Slovenia adopted net neutrality laws in 2011[9] and 2012[10], and then several additional European countries started to consider similar regulatory measures. On the other hand, other countries used self-regulatory approaches and/or based their approach on transparency while effectively allowing throttling and blocking of applications over the Internet access. [11]

On this background, with a significant level of restrictions on Internet access for European citizens, and an increasing variation in regulation of net neutrality among member states, the European Commission proposed a new net neutrality regulation in 2013. Following the law-making process of the European Union, net neutrality rules were finally adopted by the end of 2015.[12]

1.1 Regulation vs. Guidelines

The European net neutrality rules entered into force 30 April 2016. This Regulation has a solid legal basis, established through the European democratic law-making process.

[5] Regulatory framework (2009)
[6] van Schewick (2014)
[7] BEREC (2012)
[8] Norwegian Communications Authority (2009)
[9] Dutch Telecommunications Act (2011)
[10] Slovenian Electronic Communications Act (2012)
[11] European Commission (2014)
[12] Regulation 2015/2120

The Regulation is seeking to safeguard equal and non-discriminatory treatment of Internet traffic and related end-users' rights, such as the right to access and distribute information.[13] This describes in other words "net neutrality" as the goal. Interestingly, in the corresponding recital of the Regulation, preservation of the Internet ecosystem as an engine of innovation is explicitly included among the goals.[14]

The operational parts of the Regulation cover commercial conditions, such as speed and volume, but also other commercial practices, where many will consider zero-rating[15] to be the typical example. Furthermore, different technical practices are covered; reasonable traffic management, exceptional traffic management and specialised services.

According to the Regulation, BEREC is given the mandate to develop Guidelines for regulators' implementation of the Regulation.[16] In this regard, it is important to note that BEREC's Guidelines do not create any new rules; they only providing guidance on the regulatory implementation of existing rules. Furthermore, national regulators shall conduct supervision and enforcement of the Regulation, and also publish reports on an annual basis on their monitoring and findings.[17]

Below some of the aspects covered by the Regulation and BEREC's Guidelines are discussed, with particular regard to Article 3 which is titled "Safeguarding of open internet access".

2. Zero-rating and net neutrality

Zero-rating is an increasingly important aspect of the net neutrality debate. Zero-rating has similar effects as technical traffic management, constituting an application-specific measure, influencing end-users' control over their own access to the Internet, as well as raising entry barriers for CAPs. This is of particular concern for European CAPs competing with larger US-based CAPs.

An often heard argument is that zero-rating ensures cheaper access to the Internet for low-income consumers. But the basis of comparison should not be absence of cheaper offers. In fact, ISPs concerned about price-sensitive consumers can provide neutral low-cost/low-speed service offers, possibly with an additional data allowance corresponding to the zero-rated data volume, which the consumer can use flexibly.

It is advantageous to not pay for some amount of traffic, and this is clear when asking consumers about the immediate perception of zero-rated offers.[18] But to detect consumers' fundamental view about this, one should instead ask them whether they would prefer an ordinary zero-rated offer or an offer where they can control themselves how to use the additional data allowance.

Another major limitation with consumer surveys is that it is difficult to assess long term effects in the market based on these. Long term effects are typically the effects on entry

[13] Regulation 2015/2120, Article 1

[14] Regulation 2015/2120, Recital 1

[15] Zero-rating means that the ISP charges a price of zero for the traffic associated with a particular application or applications, and that the data does not count towards any data cap in place on the Internet access service.

[16] Regulation 2015/2120, Article 5(3)

[17] Regulation 2015/2120, Article 5(1)

[18] However, research has shown that consumers are interested in zero-rated applications mainly when data allowance is low. See BEREC (2015)

barriers to start-ups and innovation of new applications. New applications could become a major advantage for consumers in the future, as we have seen already on the Internet in the past.

It is probably possible to construct examples where zero-rating has good effects for end-users, but the market requires clear rules to avoid regulatory uncertainty. Therefore one should be careful when considering targeted examples, and one should instead take an overall view when drawing general conclusions about regulation of zero-rating.

In the later years, observers have argued that the challenge to net neutrality has shifted from throttling and blocking of applications over to zero-rating of applications.[19] In other words, some ISPs are moving from *technical* discrimination of traffic to *economic* discrimination, where some traffic is cheaper or free to transmit over the network than other traffic.

Even though traffic may not be prioritized from a technical point of view, end-users would be incentivised to select applications from specific CAPs[20], steered by the decisions taken by their ISPs. Smaller CAPs, start-ups and non-commercial content providers will typically not receive the same advantage. This would harm the users' free choice and freedom of expression.

Furthermore, to be able to be zero-rated, CAPs would have to engage with ISPs around the world, which would represent and economic burden that may be particularly difficult to bear for small-and-medium-size CAPs. This is a significant hurdle compared to an open Internet, where any application is sharable from a single access. Therefore, zero-rating is likely to raise the barrier for start-ups entering the market, becoming an obstacle to "innovation without permission" which should be safeguarded by net neutrality.

2.1 Regulatory assessment of zero-rating

Commercial practices, and zero-rating in particular, have been surrounded by some uncertainty in the European discourse on net neutrality, and the opinions have been strong on both sides.[21] Law-makers have chosen a middle course regarding zero-rating and other commercial practices in the Regulation, and such practices are neither explicitly allowed nor explicitly prohibited.

Article 1 affirms that "This Regulation establishes common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of Internet access services and related end-users' rights." In the following detailed provisions, end-users rights are described, followed by equal and non-discriminatory treatment of traffic. The former is discussed in this section, while the latter is discussed further below.

End-users' rights are defined in Article 3(1): "End-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service."

[19] Digital Fuel Monitor (2014)
[20] See e.g. BEREC (2016a), paragraph 48
[21] See e.g. BEREC (2016b)

Furthermore, Article 3(2) explains that agreements on commercial and technical conditions, as well as any commercial practices “shall not limit the exercise of the rights of end-users laid down in paragraph 1”. It is under these provisions that the commercial practices, including zero-rating will be assessed. In case technical practices are intertwined with commercial practices, provisions regarding technical practices still apply.

Therefore, based on the Regulation’s ban on technical blocking and throttling of applications[22], BEREC’s Guidelines recommend to prohibit zero-rating practices where the zero-rated applications receive preferential treatment after the data cap is reached, e.g. where the zero-rated application is still accessible, while other applications are blocked.[23]

For more complex cases, BEREC recommends general assessment criteria which national regulators can use to assess commercial practices in general, including zero-rating. These criteria encompass market positions of the providers involved, covering ISPs and CAPs, the scale of the practice, effects on end-user, including effects on CAPs, and whether the general aims of the Regulation are circumvented.[24]

When conducting such assessment, regulators may take into account several aspects, according to the Guidelines. Commercial practices that have similar effects as technical blocking are likely to be limiting the exercise end-users rights. Practices that apply a higher price to specific applications are likely to do the same, while the possibility of higher prices for applications may also discourage innovation. Practices that apply a lower or zero price, will incentivise end-users to use zero-rated applications, and the lower the data cap is, the stronger such influence is likely to be.[25]

Due to such case-by-case approach, national regulation in this area may vary to some extent across Europe, and BEREC’s Guidelines can’t provide the same level of regulatory certainty as for other areas. Upcoming cases of zero-rating will need a comprehensive assessment by national regulators. The Guidelines provide criteria for the regulatory assessment, but in particular the earliest cases may be complex to settle. Over the coming years, regulators’ experiences will show how well this methodology eventually works.

3. Different levels of traffic management

Traffic management refers to any technical measures used to forward traffic though the networks. In modern IP-based communication networks, the packet switching enables rather flexible allocation of capacity for the different communication sessions. Such traffic management measures vary from simple first-come-first-serve handling of packets, to more or less sophisticated scheduling of packets belonging to the different communication sessions.[26]

When assessing traffic management practices for Internet communications, the European net neutrality rules define three different levels of traffic management. The *ground level* is when Internet traffic is treated agnostic to applications and endpoints generating the traffic, which is described in the 1st subparagraph of Article 3(3). The two next levels contain

[22] Regulation 2015/2120, 3rd subparagraph of Article 3(3)
[23] BEREC (2016a), paragraph 41
[24] BEREC (2016a), paragraph 46
[25] BEREC (2016a), paragraph 47
[26] See for example BITAG (2013)

reasonable traffic management described in the 2nd subparagraph, and *exceptional* traffic management described on the 3rd subparagraph of Article 3(3). (Note that this categorization does not align with the ones used in other regulations, e.g. FCC open Internet rules[27].)

Traffic handling on the Internet is referred to as "best effort"[28], reflecting the fact that Internet communication does not provide any guaranteed quality levels. However, ISPs can provide relatively good quality through proper operation of their networks. The "weak link" will be the capacity provided towards interconnected ISPs, since communication in many cases is performed across several ISPs' networks. However, this can to some extent be mitigated by the interconnection agreements with peering and transit ISPs.

When Internet traffic is transmitted together with specialised services over a shared infrastructure, which often is the case, regulatory assessment of the net neutrality rules also takes into account *overall* traffic management practices. Such traffic management is related to how traffic from specialised services is handled in parallel with traffic from Internet communications. In the European Regulation, this is described in Article 3(5).

The main question when specialised services come into the picture will typically be whether network capacity is sufficient to avoid a detrimental effect on the quality of internet access services. Regulations may, as in the European case, set out requirements in this regard. The next question will then be *how* sufficient capacity is ensured, and in particular how ISPs ensure that specialised services don't degrade Internet communications. The assessment of traffic management related to specialised services is further discussed in section 4.

In the three subsections below, the different types of traffic management related to Internet access services are discussed in the context of the European net neutrality Regulation.

3.1 Ground level of traffic management

The Regulation establishes common rules "to safeguard equal and non-discriminatory treatment of traffic"[29]. Traffic can normally be considered to be treated equally as long as packets are processed agnostic to sender and receiver, to the content accessed or distributed, and to the application used or provided. This constitutes the ground level of traffic management, usually referred to as "best effort". However, this may not necessarily lead to identical network performance and quality of service (QoS) for all end-users.[30]

A less well-known but fundamental functionality of the Internet technology is *endpoint-based congestion control*.[31] This works as a feedback-based adjustment of the transmission rate at which packets are sent into the network by endpoints, applied to relieve the congestion in the network. Note that endpoint-based congestion control is separate from network-internal congestion management discussed in subsection 3.3.

Applications use transport layer protocols when IP packets are transmitted into the network. Traditionally, two different transport layer protocols are used on the Internet, TCP and UDP, and this has been supplemented with other alternatives the later years. The transport layer

[27] FCC (2015)

[28] Best effort is further discussed in section 2.1

[29] Regulation 2015/2120, Article 1

[30] BEREC (2016a), paragraph 53

[31] IETF (2010a)

protocol used may, and often does (as in the case of TCP), execute congestion control in the endpoints, as described above. However, UDP does not support congestion control.

When the traffic load on the network increases beyond the available capacity, packets start to get queued in the network nodes. If the traffic load continues to increase, the queues eventually get filled, and packets start to become dropped. Packet drops can therefore be interpreted by endpoints as a signal about congestion in the network. TCP traffic flows are responsive to such signals and "back off" during congestion. When congestion disappears after a while, traffic sources start to speed up again.[32]

An interesting example of congestion control for ongoing development of applications is related to *Web Real-Time Communication*, WebRTC[33]. WebRTC is a relatively new standardised telephony application architecture executing in web browsers. A dedicated congestion control scheme, RMCAT,[34] is developed for the WebRTC architecture to limit the congestion due to the anticipated increase in real-time communication. This example illustrates the adaptability of the congestion control functionality to accommodate new needs in Internet communications.

BEREC's net neutrality Guidelines explicitly recognise endpoint-based congestion control as a legitimate measure under equal treatment of traffic.[35] This is due to the fact that such mechanisms are executing in the terminal equipment together with the application software, as opposed to functionality implemented inside the ISP's network. This is also in line with the end-to-end principle, since the congestion control is running in the endpoints connected to the Internet.

3.2 Reasonable traffic management

The requirement to treat traffic equally does not prevent ISPs from applying *reasonable* traffic management for Internet traffic, as a second level of traffic management. Note that the concept "reasonable traffic management" in the European net neutrality Regulation is a narrower concept than in many other jurisdictions, such as FCC's open Internet rules. An important criterion for reasonable traffic management is that it is based on objective technical QoS requirements, such as latency, jitter and packet loss. Furthermore, such measures shall not monitor the specific content of the traffic.[36]

An essential aspect of reasonable traffic management is the feature "*categories of traffic*" introduced by the European net neutrality Regulation. As the Regulation explains, categories of traffic are defined based on "objectively different technical QoS requirements". Furthermore, BEREC's Guidelines explain that this may be linked to applications, but it is anyway the QoS requirements that provide the basis for the categorisation. An important requirement in this regard is that applications with equivalent requirements are handled agnostically within the same category.[37]

Differentiating traffic by treating packets based on objective, technical reasons with a goal to optimise *overall* transmission quality would thereby be allowed. However, reasonable traffic

[32] IETF (2015b), Section 2

[33] W3C(2016) and IETF (2016a)

[34] IETF (2016b)

[35] BEREC (2016a), paragraph 54

[36] Regulation 2015/2120, 2nd subparagraph of Article 3(3)

[37] BEREC (2016a), paragraph 66

management is not allowed to throttle or block specific applications.[38] Furthermore, such measures should be clearly distinguished from specialised services where optimisation may be performed in order to meet requirements for a *specific* level of quality for that service.[39]

The Regulation requires that any implementation of categories of traffic does not monitor "*specific content*".[40] This term is explained in BEREC's Guidelines to be understood as "transport layer protocol payload".[41] However, this still allows for identification of QoS requirements of individual IP packets based on IP header and transport layer protocol header, and this information will also be available in case transport layer protocol payload is encrypted.

If an ISP implements "categories of traffic" in the network, the general transparency requirements of the Regulation should ensure that end-users, including CAPs, receive sufficient information to run their applications according to the ISPs' traffic categories. This may contribute to a feasible approach for a QoS architecture which takes both ISPs' and CAPs' needs into account. A well-known approach to user-controlled QoS is proposed by Barbara van Schewick.[42]

An ISP's reasonable traffic management is relying on information in IP and transport layer protocol headers, and this information is ultimately provided by the applications sending packets into the network. As expressed by recital 9, ISPs' traffic management measures are "responding to" the QoS requirements of the categories of traffic. In principle, this encompasses an application-controlled/user-controlled aspect, since the content of the traffic will necessarily have to be provided by the end-users' applications.[43]

A potential way of implementing reasonable traffic management may be to base it on IETF DiffServ architecture[44], where each DiffServ class corresponds to a "category of traffic". Packets belonging to each DiffServ class could be identified based on the information available in the header as described above. However, the concrete implementation would of course have to be done in line with the net neutrality Regulation.

3.3 Congestion management and exceptional traffic management

As a third level of traffic management, exceptional traffic management *going beyond* reasonable traffic management may be used under stricter conditions. For this purpose, the Regulation specifies these exceptions: (a) other legislative measures; (b) network integrity and security; and (c) congestion management. Only under these three exceptions, measures such as throttling or blocking of applications are allowed. [45]

In this subsection the focus is on *congestion management*, since this is a particularly complex traffic management measure to implement, and therefore also complex to assess.

[38] BEREC (2016a), paragraph 74

[39] BEREC (2016a), paragraph 75

[40] Regulation 2015/2120, 2nd subparagraph of Article 3(3)

[41] BEREC (2016a), paragraph 70

[42] van Schewick (2015)

[43] See also BEREC (2016a), paragraph 64

[44] IETF (1998) and IETF (2015)

[45] Regulation 2015/2120, 3rd subparagraph of Article 3(3)

As BEREC's Guidelines describe, congestion management may also be done on a general basis, independent of applications. In light of the principle of proportionality, regulators should consider whether such *application-agnostic* congestion management would be sufficient and equally effective to manage congestion, when assessing ISP's practices.[46]

Mitigation of network congestion was discussed above under the section concerning equal treatment of traffic, where endpoint-based congestion control was presented. The result of such congestion control functionality is that the different communications sessions reach a state of dynamic equilibrium[47] which shares the available network capacity between different traffic sources.

Traffic management measures with different strengths, or level of intrusion, may be used to mitigate congestion in networks, and these levels of traffic management are relevant to assess based on the proportionality criterion. First, the full potential of endpoint-based congestion control should be investigated. Second, network-internal mechanisms of ISPs which *assist* endpoint-based congestion control should be examined. Finally, regular network-internal congestion management should be considered.

1. As described in section 3.1, endpoint-based congestion control is not used for all traffic sources, and increasing deployment of up-to-date software in terminal equipment is prerequisite for this functionality to provide adequate avoidance of congestion. Therefore, the usage level of well-behaving congestion control is relevant.

2. The simplest congestion control functionality responds to packets that are dropped at the end of queues in network nodes, so-called "tail drop". Network-internal mechanisms can be added to *assist* the congestion control function in the endpoints. Such complementary functions are called Active Queue Management (AQM), and they can signal congestion in a more intelligent way to endpoints.[48] An important criterion in relation to equal treatment of traffic is that such mechanisms are agnostic to the applications running in the endpoints.[49]

   If "categories of traffic" are implemented by the ISP in the network, AQM may differentiate between traffic belonging to the different categories based on the QoS requirements of each category.[50] In that regard, the general assessment criteria for reasonable traffic management apply,[51] as described in section 3.2 above.

3. Finally, regular network-internal congestion management functions may be implemented by ISPs. Such measures can be either application-agnostic or application-specific, where the former would be less intrusive than the latter. Regarding the former type, some variants are currently available[52], but this is also an area for further research. The latter type would typically involve deep packet inspection (DPI)[53].

[46] BEREC (2016a), paragraph 92

[47] Huston (2015)

[48] IETF (2015a)

[49] BEREC (2016a), paragraph 54

[50] IETF (2015a), section 2.1

[51] BEREC (2016a), paragraph 65

[52] IETF (2010b) and IETF (2012)

[53] Deep packet inspection (DPI) is traffic monitoring that inspects IP packets beyond the transport layer header. Refer also to EDPS (2011)

> *Application-agnostic* measures would be considered to be “equal treatment”, as described previously. Moreover, based on the 3rd subparagraph of Article 3(3) the Regulation which says that exceptional traffic management should not be applied “except as necessary, and only for as long as necessary”, one could challenge whether *application-specific* congestion management would be necessary when application-agnostic alternatives exist, depending on how effective the different measures are.[54]

The conclusion that can be drawn from this discussion is that there are several softer measures to mitigate congestion that should be considered, before considering application-specific congestion management as necessary. As BEREC’s Guidelines say, “When assessing congestion management exceptions under letter (c), NRAs should refer to the general criteria of strict interpretation and proportionality set out in Article 3(3) third subparagraph. Furthermore, NRAs should check that congestion management is not used to circumvent the ban on blocking, throttling and discrimination.”[55]

4. Specialised services

Specialised services, denounced by some, praised by others, are also covered by the Regulation and by BEREC’s Guidelines. These services are other services than Internet access services that may be offered by providers under certain conditions. The first main condition is that the service is offered to meet requirements for a specific level of quality which can’t be achieved over the Internet access service, and the second main condition is that the network capacity is sufficient to provide the service in addition to any Internet access service provided.[56]

Regarding the first main condition, which is introduced by the 1st subparagraph of Article 3(5), this also works as a kind of definition of the term “specialised services”. BEREC’s Guidelines uses the term as a short expression for “services other than internet access services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality”.[57]

Furthermore, the Guidelines provide a few examples of specialised services, such as specific types of VoIP and IPTV[58], but are carefully avoiding “freezing” the interpretation of the concept. Through Article 3(5) of the Regulation, providers are maintaining the opportunity to provide services with QoS requirements, and the role of the regulators is not to foresee which services these could be, but to supervise the safeguarding of the Internet access service.

Specialised services ensure “compatibility” between the European net neutrality Regulation and provision of services with QoS requirements e.g. in 5G networks. As the 5G Manifesto from European industry says, “A fundamental enhancement brought by 5G is the possibility to deliver virtual ‘network slices’ offering different capabilities according to specialised needs. 5G network slices are meant to run on shared infrastructure without deteriorating

[54] BEREC (2016a), paragraph 92
[55] BEREC (2016a), paragraph 90
[56] Regulation 2015/2120, Article 3(5)
[57] BEREC (2016a), paragraph 2
[58] BEREC (2016a), paragraph 113

the agreed levels of service."[59] Specialised services and Internet access can thereby coexist in mobile infrastructure.

Regarding the second main condition about sufficient capacity which is introduced by the 2nd subparagraph of Article 3(5), it is essential that the Regulation's goal is to safeguard the Internet access service, and not the specialised services. As the Regulation says, the ISP may offer specialised service "only if the network capacity is sufficient to provide them in addition to any internet access services provided".[60]

On the other hand, implementation of specialised services will have their own inherent "protection mechanisms" based in the QoS architecture used by the ISP. This is the nature of the specialised services. Specialised services should under no circumstances be provided at the expense of Internet access services.

According to the Regulation, in fixed access networks the access speed shall be relatively precisely defined. Furthermore, both based on ISPs' information, and based on regulators' measurements, the performance of the Internet access service can be monitored to check whether it is degraded or not.[61]

In mobile access networks it is more challenging to check potential degradation of Internet access services. Both ISPs' information and regulators' measurements will need particular attention for regulators to fulfil their obligation to "closely monitor and ensure compliance" in the case of mobile Internet access. [62]

5. Concluding remarks

Summing up, the European net neutrality rules are based on a democratic law-making process, providing a solid basis for regulation of net neutrality the next years. However, due to the novelty of the rules, there will most probably be challenging questions to resolve. With a view to preserve the value of the Internet for upcoming generations, it is important to continue the work to maintain the net as an open and non-discriminatory platform for everyone.

The current high-profile net neutrality question about zero-rating has not achieved a clear answer under the European net neutrality Regulation. However, a general assessment methodology is provided, with a possibility for national regulators to intervene if necessary. Over time the development of the market under this regulatory regime will gather experiences that can be used to feed into any future legislative processes.

The discussion in this paper shows that the European net neutrality Regulation provides a framework which is compatible with the technology evolution. On the one hand the traffic management measures cover traditional best effort communications, advanced congestion handling, and potential class-based QoS architectures. This includes a user-controlled aspect of such QoS architecture, which has an interesting potential.

On the other hand, the Regulation allows provision of specialised services in parallel with Internet communications, which facilitates experimenting with different business models.

[59] 5G Manifesto for timely deployment of 5G in Europe, July 7th 2016

[60] Regulation 2015/2120, 2nd subparagraph of Article 3(5)

[61] BEREC (2016a), paragraph 121

[62] BEREC (2016a), paragraph 123

This may show particularly interesting for mobile access networks, where the upcoming 5G network architecture emphasises QoS-based services, at the same time continue today's use of mobile access networks to provide Internet access services.

The conditions for net neutrality in Europe and related regulatory measures should over time be reconsidered based on how commercial and technical practices develop. In case zero-rating practices should distort the market and reduce end-users' control over their own Internet use and raise entry barriers for CAPs, this may spur clearer rules of such commercial practices.

Tension between Internet-based communication and specialised services may evolve over time. The European net neutrality Regulation prescribes obligations on national regulators to "closely monitor and ensure compliance" with the Regulation, whereby this evolution will be scrutinised, and corrective regulatory measures may be launched if necessary.

References

BITAG, 2013, Real-time Network Management of Internet Congestion

BEREC, 2012, Traffic Management Investigation, http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/?doc=45

BEREC, 2015, How do consumers value net neutrality in an evolving Internet marketplace? BoR (15) 65

BEREC, 2016a, BEREC Net Neutrality Guidelines, "BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules", http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6160-berec-guidelines-on-the-implementation-b_0.pdf

BEREC, 2016b, BEREC consultation report on BEREC Net Neutrality Guidelines, "BEREC Report on the outcome of the public consultation on draft BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality rules", http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6161-berec-report-on-the-outcome-of-the-publi_0.pdf

Digital Fuel Monitor, 2014, List of 75 zero-rated, potentially anti-competitive mobile applications/services, violating net neutrality, http://dfmonitor.eu/insights/2014_oct_zerorate/

Dutch Telecommunications Act, 2011, Article 7.4a, https://www.unodc.org/cld/document/nld/1988/telecommunications_act_of_the_netherlands.html

European Commission, 2014 Report on Implementation of the EU regulatory framework for electronic communications, https://ec.europa.eu/digital-agenda/en/news/2014-report-implementation-eu-regulatory-framework-electronic-communications

EDPS, 2011, Opinion of the European Data Protection Supervisor on net neutrality, https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-10-07_Net_neutrality_EN.pdf

FCC, 2015, Report and order on remand, declaratory ruling, and order, FCC 15-24

Huston, Geoff, 2015, TCP Protocol Wars, Internet Protocol Journal, Volume 18, Number 2

IETF, 1996, RFC 1958, Architectural Principles of the Internet

IETF, 1998, RFC 2475, Architecture for Differentiated Services (DiffServ)

IETF, 2010a, RFC 5783, Congestion Control in the RFC Series

IETF, 2010b, RFC 6057, Comcast's Protocol-Agnostic Congestion Management System

IETF, 2012, RFC 6789, Congestion Exposure (ConEx) Concepts and Use Cases

IETF, 2015a, RFC 7567, Recommendations Regarding Active Queue Management

IETF, 2015b, RFC 7657, Differentiated Services (Diffserv) and Real-Time Communication

IETF, 2016a, Real-Time Communication in WEB-browsers (RTCWeb) working group, https://datatracker.ietf.org/wg/rtcweb/charter/

IETF, 2016b, RTP Media Congestion Avoidance Techniques (rmcat) working group, https://datatracker.ietf.org/wg/rmcat/charter/

Norwegian Communications Authority, 2009, Norwegian guidelines for net neutrality, http://eng.nkom.no/technical/internet/net-neutrality/net-neutrality/_attachment/9222?_ts=1409aa375c1

Regulation 2015/2120 of the European Parliament and of the Council, 25 November 2015, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32015R2120

Regulatory framework 2009, Regulatory framework for electronic communications, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3Al24216a

Slovenian Electronic Communications Act, 2012, http://www.uradni-list.si/_pdf/2012/Ur/u2012109.pdf#!/u2012109-pdf

van Schewick, Barbara, 2010, Internet Architecture and Innovation, MIT Press

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

van Schewick, Barbara, 2015, Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like, https://law.stanford.edu/publications/network-neutrality-and-quality-of-service-what-a-non-discrimination-rule-should-look-like-2/

W3C, 2016, Web Real-Time Communications Working Group, https://www.w3.org/2011/04/webrtc/