Net Neutrality Under EU Law – a Hindrance to 5G Success

Raimo Kantola
Aalto University
raimo.kantola@aalto.fi

Abstract: EU has adopted a law on Net Neutrality (NN) ruling that Internet access providers should treat all traffic equally irrespective of sender, receiver, content, service, application or device in use. The 5G community is developing a network that can be tailored to a use case, meaning that it intends to treat traffic differently for each use case. Tailoring can be at least in terms of traffic management, allocated types and amount of resources, redundancy, particular forms of security etc. Moreover, 5G network uses network function virtualization, i.e. cloud technology is applied to run the network itself while the law on NN does not mention the concept of the cloud. The interpretation is that if a cloud platform is owned by the Internet access provider, the cloud is just a part of the network and under the NN regulation. At the same time if a cloud-based computer is owned by a cloud or content provider, it is a terminal and thus not regulated. 5G introduces the idea of edge computing (EC) that can use virtualization and allows special treatment for some applications or services. So, in addition to just transmitting packets, 5G can process them in the "compute" elements. This paper explores how significant is this controversy between the new concepts of networking in 5G and the EU regulation and what is its possible impact on the network providers. The paper studies to what extent and how the 5G ideas can be applied under the EU law and whether something should be done about the law and in particular the Guidelines that have been published by the Body of European Regulators for Electronic Communications (BEREC) to clarify the implementation of the law. Finally, we discuss the possible impact of the law on industry structure.

Keywords: Net neutrality, 5G, slicing, traffic treatment, traffic management, security, specialized service.

1. Introduction

EU parliament adopted a law on open Internet or Net Neutrality (NN) in 2015 [1] and assigned the Body of European Regulators for Electronic Communications (BEREC) to provide guidance to the national regulatory authorities (NRA) in implementing the law. BEREC issued the corresponding guideline document in 2016 [2]. Wider background of the regulation is discussed in [3]. The law intends to protect and defend end user choice and maintain innovation of services and applications that make use of the Internet. The EU law on NN says that provider of Internet access services (IAS) should *treat all traffic equally*, without discrimination, restriction or interference, irrespective of *sender, receiver, content, service, application* or the *device* in use. The law sets itself a requirement of being neutral to technology. Provided that we can define "traffic" as any information flow carried over the network for any type of service irrespective of the format, the law adheres to this ideal by always talking about "traffic treatment". We assume that IAS can be provided by Mobile Network Operators (MNO) or Internet Service Providers (ISP). It would seem reasonable to assume that the requirement of equal traffic treatment applies no tighter than the human timescale i.e. anything less than human reaction time is irrelevant. However, this is not discussed in the law or the Guidelines.

The Guidelines [2] starts by talking about "traffic treatment" but then almost in midsentence in Article 3.3, item 53 switches to discussing "packet treatment". Packet treatment is a well-known term in Internet Requests for Comments (RFC) on Differentiated Services. In RFCs packet treatment refers to a per-hop behaviour indicated by the DiffServ Codepoint (DSCP) value in the IP packet header. In literature "packet treatment" applies in packet timescales, for example on 10 Gbit/s an average packet of 500 octets lasts for 0,4 microseconds. Clearly, this term is technology dependent. It is also reasonable to ask, what business relevance are such timescales?

The Guidelines go on to specify that "best effort" which is indicated by one of the codepoints in the DSCP field of the IP header is a *standard* and that any deviation from that standard is allowed if it is *necessary or objectively necessary* and justification for it can be found in the regulation. This follows from the structure of the regulation that all deviations from the equal treatment must be mentioned in the regulation. Nevertheless, item 63 in the Guidelines discusses the possibility that IAS implement quality of service, i.e. use more than just one of the DiffServ codepoints to handle *objectively different categories* of traffic.

The Guidelines talk about *specialized services* that allow deviating from the requirement of equal treatment. The interpretation of what qualifies as a specialised service is open. That they cannot replace Internet access services is clearly mentioned.

Guidelines mention that machine-to-machine communications is out of scope of the NN requirements, VPNs are allowed and some provisions have been made for *network security*. A generic rule of the exceptions is that the special treatment must be *objectively necessary*.

The NN idea of equal treatment is opposed to what 5G is proposing, namely tailoring the network for a use case. Tailoring for a use case could be in terms of traffic and packet treatment, i.e. traffic management, particular types of security processing, the amount of link and compute resources allocated to the use case, redundancy etc.

Since the NN and the idea of 5G seem to be in conflict, this paper will analyse this issue in some detail with the target of finding out whether the EU NN will be a hindrance or a show stopper to 5G investments and innovation, what the industry should try to do if that is the case and what is the wider impact of EU NN onto the industry structure.

2. Related Work

The combination of net neutrality and 5G has not attracted many works so far. A search in IEEEexplore with the two key words gives just one paper [4]. The paper [5] is an early attempt to address the very issue we are trying to analyse. The paper in particular looks at 5G network slicing and its relation to specialized services mentioned in EU regulation [1,2]. The focus is on intelligent resource sharing mechanisms and Quality of Service that is needed for certain specialised services. The paper does not address security and only touches the industry level impact of NN. The paper brings nicely forward the argument that best effort is not necessarily best always and that smart resource sharing created a leap in computing by introducing cloud computing and that we need to expect similar effect from Network Function Virtualization if NN regulation does not prevent it.

The term network neutrality was popularised by Tim Wu in his seminal paper [6] in 2003. The paper focused on the issue of equal treatment of applications for the purposes of boosting innovation on applications and through this maximizing customer choice. The paper argues that one cannot have both equal treatment of applications and equal treatment of packets because IP inherently favours data traffic and is not great at handling low delay interactive applications. The idea of NN itself is older. Issues of competition and constraining the misuse of market power preceding Wu's paper included the battles of new ISPs versus traditional telecom companies that also wanted to become ISPs.

In literature we find both papers that are in favour of NN, e.g. [7] and offer criticism [8, 9, 10]. Schulzrinne [8] reasonably argues that NN is not about packet treatment but about money. Maillé et.al [9] demonstrates that even if regulation goes to the level of packets, networks can still favour some applications over others. The paper [9] argues that it is time to extend the NN discussion to cover the whole Internet value chain including such new elements as Content Distribution Networks or search engines. Discussing cyber security, a paper [10] demonstrates that "Net neutrality protects both ordinary users and actors with hostile intent". Discussing regulation, V. Cerf ends his paper [11] with "Social and legal norms may be the means by which we achieve collaborative intervention against harmful behaviors on the Internet. Protocols are a form of cooperation and perhaps it is now time to invent new diplomatic protocols, aided by technology, to fashion an Internet worthy of persistence and global access" showing that even the founding father of the Internet is ready to discuss going beyond "best effort" that is declared "standard" in the EU regulation.

In the Guidelines [2], item 63 seems not to allow a paradigm shift in QoS proposed in [12] because the proposal does not require that particular QoS would be objectively necessary, rather user choice is enough to choose a quality class. A recent report [13], however, considers the use of network slicing introduced in 5G in a way that may allow quality that is provided by user choice with no reference to whether the particular quality is necessary or objectively necessary so long as the QoS classes are application agnostic. The argument is that each quality class is its own Internet access service and that an IAS can sell many of them to a single customer. Whether this interpretation is supported by BEREC is unclear. So much is clear that BEREC allows selling services of different quality class e.g. in terms of access speed and delay.

The ideas of virtualization of computing and cloud computing are older than the law on NN. In 2006 Amazon started offering commercially cloud services. By using the cloud, companies are able to save significant amounts of money on information technology (IT). In 5G the networking and mobile industry has embraced the cloud technology and may use it e.g. to build more affordable networks that target giving the users services that give a perception that network capacity is infinite and there is no waiting time for any information to be presented to the end user. Let us call this last property the “instant Internet”. A significant difference to older networks is that the network itself is not just about transporting packets but it contains compute elements to be used to give the perception of instant Internet. This compute function in 5G is called multi-access edge computing or mobile edge computing. For simplicity we will call it just edge computing assuming that this has at least two alternative implementations, one where the compute element is inside the mobile network e.g. as a part of a master base station and another where the compute element is logically in the Internet but at a low transmission distance from the end user giving a millisecond level round trip delay between the user and the edge compute node. The 5G R&D community believes that achieving the kind of low latency needed e.g. for augmented reality applications, the local “compute” function will be used in an application dependent manner.

5G also offers very high bitrates to the end devices. If the data flow is from a cloud-based server to the device, this leads to extremely high capacity demand on the 5G to Internet interconnection to the boundary of what is feasible with the current technology in networks with hundreds of millions of customers. Since most of the content carried is video, it would be possible to download most of the videos just once and feed them to the devices from a local “compute” element e.g. by stretching the content distribution network to the local “compute” element.

Cloud computing, when applied to network function virtualization, allows among other things building network functions that are user specific and fully under the user’s control. This has never been possible during the era of building networks from vertically integrated boxes whose hardware and software are both supplied by the same vendor.

3. Content favouring on the net

Even before the adoption by the EU of the NN regulation, the old battle lines between operators and over the top (OTT) providers had shifted due to the introduction of Content Distribution Networks (CDN). These can be used by the content providers to ensure high quality delivery of their content to the end users. The implication is that content has been dropped from the list what networks really treat equally. The end users do not care where the favouring took or did not take place, the ISP network or the CDN. The regulation does not address this issue at all because CDNs and cloud services are not in the scope of the regulation.

All advertisement financed services such as Facebook and Google run algorithms that segment the users to fine grained groups that are then used by the advertisers (who are the customers) to push advertisements to the users who might be interested in them. While we talk about selling goods this may sound like a benign thing to do. But those services classify *all content* accordingly by user groups and by popularity, i.e. how many people clicked on them. This includes politics, all false and true theories about any subject. The essence of this approach is to tell people what they want to see and hear. It is also known that lies attract more clicks than true stories. In this approach all content is treated differently rather than equally. The result is that people tend to isolate themselves into likeminded bubbles and they seize to meet and understand other points of view. Lots of people are trapped in bubbles of false theories and lies. The system can also be played to offer very targeted political message to every group like it was done in the last US presidential election in 2016. This raises a strong argument that private monopoly cloud providers such as FB and Google are posing a threat to democracy and that their algorithms oppose freedom of speech. A wider analysis of the detrimental impact of FB, Google and Amazon on culture is presented in [14]. However, NN is doing nothing to address these very real issues while the regulators attention is focused on 20-year old battle lines. Since the real networks do not treat content equally, may be this aspect should be dropped from the regulation? Alternatively, cloud services such as Facebook and Google could be regulated as well?

4. 5G technology and its use cases

5G is expected to offer high capacity to consumers, i.e. enhanced mobile broadband services (eMBB) that can for example be offered as a replacement of fixed broadband services with the added bonus of being available everywhere. In addition, 5G will support massive Internet of Things or machine-to-machine communications (MTM) to connect billions of sensors to the network and finally ultra-high reliability and low latency communications (uRLLC) for example for the Industrial Internet. This variety of use cases is the justification for network tailoring being a cornerstone of the 5G networking architecture. It is assumed that within the MTM and uRLLC categories there will be many use cases with rather local, country wide or even regional (such as European) coverage. These fall to the so-called vertical market segments that complement the consumer markets for MNOs.

5G is expected to be software defined, meaning that the control and data planes are separated. The network functions such as mobility management, session management, the gateway to the Internet or the firewall are virtualized, so they run in virtual machines on a cloud platform most likely owned by the MNO. Some of these functions need to be rather close to the end user and will not work well if run on a remote cloud. In addition, the 5G network will have extra computing capacity close to the users for processing certain types of services and applications. This compute capacity can be virtualised and we call it edge computing. It remains to be seen what is the business model of using this compute capacity, e.g. all software is supplied by the trusted network vendor and run as a part of a network-based service by the MNO or may be the compute capacity could be rented just like the cloud capacity is normally rented to any users who wish to pay. What is clear is that this area needs both technical and business innovations. *The challenge is how to find the motivation when all unequal treatment must be necessary and must be offered to all in the same way?*

A fundamental architecture principle in 5G is the idea that 5G is not a “one size fits all” network but rather the network functions can be tailored to a use case. To serve a use case, the required resources, virtualized network software and algorithms are grouped to a slice of the 5G network. A slice is similar to a virtual private network but it can span all OSI layers, include compute elements and have a dynamic geographic coverage. A device can, in principle, attach to several slices.

Slicing has raised quite a lot of enthusiasm. Players like Nokia talk about using it to serve the vertical corporate market such as Smart Grid, Smart City, support for automated driving or eHealth. It is assumed that many of the verticals have needs for low latency services that in addition have ultra-high reliability. An example of uRLLC use case is remote control over moving vehicles or remote control of cranes in a port requiring several real-time video feeds as well as tactile interfaces to the controls of the machinery. For safety reasons, such applications require very high security. Another use case for slicing would be a network for rescue services that offers dynamic coverage and capacity based on the need possibly spanning several incumbent mobile networks.

Other players [15] are much less discriminate and would apply slicing to address also consumer market needs. It seems clear that addressing the consumer market is best done if the services offer opportunities for differentiation to the operators and services providers. However, under NN, deviation from equal treatment must be necessary or objectively necessary and one can hardly offer something that is necessary as a great differentiator with its own price tag. It is rather likely that one can only offer necessary features to everyone equally. Therefore, it does not look like using slicing on the consumer markets is a new revenue source under NN lowering incentives to invest. The report [13] argues that the regulation allows offering several simultaneous Internet access services to the end user and that if the choice is made by the user, slicing could be brought to consumer markets as a means for offering quality of service. It is not clear whether this interpretation is shared by BEREC.

When all resources of a slice are isolated to an island, e.g. the Smart Grid owned and operated by an energy company in a country, the island itself can be strongly secured using not only device-based solutions but the device security can be assisted by network or cloud-based elements. Given that the underlying network is software defined, at its extreme such a *network can be a firewall*, i.e. it transports only flows that are expected and drops all other flows. The challenge is that any such secure slice is likely to need remote access from anywhere a specialist may reside at any time, i.e. the first idea is that it must be connected to the Internet that is fundamentally unsecure. This connection for remote operations may offer an attack surface to the hackers and thus the uRLLC slice would remain vulnerable. The situation can be improved by rather providing a more secure remote access to the uRLLC slice through the mobile network from a remote device with a SIM card and thus not be dependent on the Internet connection at all. In this approach, none of the nodes of a specialised network or its control centre are connected to the consumer Internet and consequently, hacked consumer devices cannot be used to attack any of the specialised network nodes or devices.

5. **Elements of contention between 5G and NN**

5.1 NN and security

All network-based security requires that some senders (hackers, bots or suspect senders) are treated differently, their packets or flows must be monitored and possibly dropped altogether. Security is mentioned in the regulation as a reason to deviate from equal treatment but *all actions must be necessary and apply equally to all users and for only as long as necessary*. User consent for filtering is not mentioned in the regulation [1, 2], so it follows that under EU law IAS are not allowed to offer e.g. parental control services to the consumers. However, contrary to EU law, some EU countries (e.g. France) make it an obligation for the operators to offer parental control. Moreover, personalised security services implemented by the IAS are not allowed by the regulation because they would imply filtering on user consent.

As a result of the NN regulation, the ISPs and MNOs are forced to a limited role in enhancing the security of the connected consumer devices with no opportunities for new revenue. The ISPs and MNOs do what the national Cyber Security Centre tells them to do but will not show any entrepreneurial attitude in network-based security services. For them security remains a cost item.

At the same time, vendors can sell to consumers any gadgets that are supposed to be connected to the Internet but have poor security. There is no such thing as compulsory security certification for consumer electronics. These devices have over the recent years been widely used by hackers as a platform for building botnets and using them for attacks. Some of these devices can be used for attacks even without hacking them (e.g. on an early Internet TV, the vendor had forgotten to remove DNS functions from Linux and it could be used as a reflector).

Cooperative cloud-based security has been proposed for 5G [16]. In an extreme *specialized services* case of cooperative security, the network becomes a firewall and it will transmit only expected flows while all unexpected flows will be denied. In [16] the security engine and framework are generic and all tailoring of security takes place by defining suitable communications security policies. The proposal [16] uses the power of cloud processing to enhance end system security. Since, the proposal of cooperative security involves ISPs and MNOs in providing value added security services, on consumer markets it comes to conflict with the NN law in Europe. At the same time most security breaches use well-known vulnerabilities on weak security devices. This threat could be addressed by the proposed cooperative, policy-based security but would be illegal under EU NN. At the same time the IAS are the only entities in the Internet value chain that could detect all hacked consumer devices and constrain their use to their intended purpose preventing all or at least most of the use for attacking other hosts on the Internet. If all devices must be treated the same by IAS, this would be clearly illegal since a few hacked hosts do not create a threat to the network itself. *As a result, NN maintains the current level of hacking on the Internet.*

NN allows any kind of security filtering on the devices that, by definition, are out of scope for NN. However, security is a function that scales poorly on battery powered devices. Also, the deployment of newest security updates is dependent on the user. So, on consumer markets, device-based security achieves the current level of security and the number of security breaches keeps growing and most of them are using known vulnerabilities. The weak security devices will remain a rich resource and platform for the hackers to utilize in their attacks. We find that NN is a *show-stopper* in solving this problem in Europe. At the same time, our desire to use the networks for ever more critical applications is unsatisfied. As we are now merging the physical and the cyber worlds, safely and security will be more and more intertwined.

5.2 Operators vs. cloud providers

One of the main justifications for regulating telecoms has been the monopolistic nature of the business giving the operator a strong gatekeeper position on the market. 5G weakens this monopolistic nature of the ISPs because the natural monopoly that has been based on the wire coming to people's homes loses its importance: 5G radio can be used as a replacement to xDSL services due to its high capacity and low delay and low jitter. Mobile markets typically have at least three competing operators, so the market may be oligopolistic but it is not monopolistic. The example of many countries shows that competition between mobile operators can work very well. At the same time, the world-wide cloud services markets are much more concentrated in a very small number of hands: Google, FB, AWS, Baidu and a few others have split the whole world into may be 3 different regions and rule supreme. It is remarkable that none of the major league cloud services providers are European. Also, a great majority of the CDN providers are American.

When a computer is owned by a cloud services provider, it can run any software without regulatory interference. The computer is a terminal similar to a device owned by the end user. If the same computer is owed by an ISP or MNO, it becomes a part of the network and its use is regulated under NN.

5G is forcing the MNOs to invest into cloud services technology. Competition in this area is ruled by economies of scale. At the same time NN regulation ties the hands of the European MNOs and will make it impossible from them to take the full advantage of the investment they anyway must make. The result is that NN paves the way for the US cloud services providers to take over all the new developments and possibly some of the core network functions that now run on MNO private platforms. This is of course unless the 5G industry manages to do something about the NN rulings. Paving the way does not imply that the cloud industry will take the battle and win. From the MNO point of view the most likely competitor from the group of cloud providers in the western word is AWS – for it the mobile networks would an extension of its hold on the logistics networks and systems. But this prospect means that parts of the regulation should be scrutinized and reviewed. In the face of the technology trend, the current ruling distorts the markets in favour of US cloud services providers.

Another justification for NN is that by banning the possibility of favouring one application over another, competition between the applications works best and will produce the most choice for the consumer. In reality what has happened is that the cloud companies like FB and Google use the advertisement-based business model, extensively mine user's privacy, profile them in numerous ways and sell this information to providers of goods and services. A lot of the application on mobile devices are also advertisement financed. Is it not time to ask: is this outcome really worthy or does it improve real consumer welfare?

5.3 The dilemma of edge computing

5G introduces edge computing (EC) that will be useful for some services and irrelevant for others. When it is applied to a service, this service will get special treatment as compared to the services that are unable to benefit from edge computing. It seems that if the NN requirement of equal treatment of packets is also applied to edge computing *only one program is allowed* on the compute platform that is supposed to run potentially any program. In the one program for all model, interactive services will suffer because the compute function will add delay while other services can benefit e.g. due to caching. Question is, how should edge computing be provided under NN? Equally for every device and own and visiting subscriber? Equally for all services even if they do not benefit from it? Or is unequal treatment in this magically fine? Would packaging to a special type of subscription be possible or even necessary in order not to break the law? Or is the idea of compute elements in the network fundamentally in conflict with NN?

Edge computing requires investment from the MNO. NN creates uncertainty how and whether the MNO is able to use it to bring in new revenue. This discourages innovation and investment. Based on oral comments from BEREC, it seems to be clarifying the rulings in this area [17]. Public hearing is expected in Fall of 2019 and the possible new rulings in early 2020.

6. Strategies for the 5G industry

6.1. Europe and the US

It is curious to note that the EU NN is clearly stricter in its requirement of equal treatment than the now abolished US law was [18]. It is curious to note that the EU law creates a great market position for the US cloud services providers against the European MNOs and that there are no European major cloud services providers. At the same time, European MNOs have lower capitalization than the US cloud services providers that have become global private monopolies that are threats to the European values of free speech and democracy. 5G offers an opportunity for the MNOs to reinvent themselves as cloud services providers. However, NN prevents the MNOs from using this opportunity while it forces them into battles for market share against US cloud companies with global reach on very unequal terms.

6.2. Baby steps

Any type of traffic or packet treatment and filtering is allowed under NN in the user device or a device in the user premises. The same applies to cloud company computers. Even if the user can do and control computations on cloud platforms in a similar isolation as on a device in user premises, since cloud computations are not mentioned in the law, they cannot be used on ISP/MNO platforms to enhance security in new ways nor can they be used to improve the service performance. It would seem a reasonable and timely upgrade to the regulation that *a virtual machine (VM) in the cloud, irrespective who owns the cloud infrastructure, should be in the same position as the user device provided that the VM is under user control.*

It seems clear that the current BEREC ruling that a cloud platform owned by an IAS is part of the network and thus under NN is not reasonable at all. Whichever way we look at it, only if the IAS can rent "compute" capacity from its platform to anyone willing to pay, at least a little fairer market can be established. There are at least two reasonable customers for the compute capacity: the subscriber and an Over-the-top services provider. The latter now install their own compute racks into IAS premises based on contracts that typically leave the maintenance of the compute rack to the IAS. These arrangements work for large IAS but the cloud providers have little incentive to make the same offer to a small IAS. If instead of physical computers, virtual machines from the IAS platform could be rented, due to better scalability of this approach compared to physical machines, a more even playing field between small and large IAS would likely appear.

An option is also that user-controlled network applications would be generically allowed. If one of such new rulings would be made, the 5G community could for example productise and deploy cooperative security for all mobile users and not only for the devices connected to the uRLLC or other specialized services slices. The result would be that devices under policy control would see only expected traffic and that the cyber-attack opportunities would be significantly reduced.

Guidelines [2] have lots of wording that can be argued to be technology dependent and thus deviate from an explicit statement of technology neutrality in the law. The main justification of having a law on NN is to boost innovation in applications and maximize end user choice. For this purpose, all this cumbersome wording about packet treatment is not needed. A minimal regulation would just say that an IAS is not allowed to favour one application over another for commercial reasons. When the regulation says that packets from all senders must be treated equally, this leads to restricting the methods than can be used to improve security using network-based algorithms. This also has limited us to the current QoS paradigm with little room for innovation.

Cloud platforms are different from network boxes in the sense that a virtual machine in the cloud can be under the user’s control or under an OTT control while this has not been feasible with the same functions implemented on integrated network boxes. Saying that if owned by the MNO or ISP, cloud is a part of the network does not increase user choice. It does the opposite by banning the users from having the best possible security for their homes and devices in the only way that really would scale on the market. Only point solutions for cloud assisted security services to security aware users using VPNs etc are possible under the current NN.

When the network technology is now taking a major step forward in 5G, this regulation is even more out of date than it was when adopted. To ensure further technology innovation for the network itself and to ensure competitiveness of European companies and the industry in 5G and cloud era, the NN regulation should be updated. More generally we need to make Europe ready for the deepening integration of the digital and the physical worlds where safety and security are much more closely related than today. This requires services like uRLLC and significant improvement of Internet security. Best effort will not be able to deliver safe integration of the cyber and physical worlds.

6.3. Strategy alternatives for the 5G industry

The industry can choose one or more of the following options. (1) it can make use of the exceptions under the NN law and the Guidelines to build *specialized services* for verticals and refine the techniques of network tailoring and virtualization. (2) The industry can lobby for clarifications to the interpretation of the NN to particular aspects of using the 5G technology such as edge computing and more generally the use of cloud technology by the MNO. This would help to alleviate the uncertainties related to investments and innovations. The industry could lobby for limited changes to the regulations such as the proposed ruling that a VM in the cloud even if the cloud platform is provided by the MNO but when the VM is under user or OTT control is out of scope of the regulation and can thus run any software. Optionally, the regulation could allow network applications, such as per user Firewalls, that provide sufficient user control over the operation. Finally, (3) the industry can lobby for repealing the law on NN arguing e.g. that there is no significant market power left to MNOs that could not be controlled under the normal market rules that ban misuse of market power in any area of the market economy.

7. **Summary**

To summarize, the EU law on NN creates uncertainties for the 5G investment and thus hampers the possibility of 5G success in Europe. It also hampers the potential success of EU based vendors on global markets since most of the rest of the world lacks such restrictive legislation and thus offers a friendly home market for non-European companies for 5G networks and network servicies. The EU law also is a show stopper to a significant step forward in Internet security needed for the era of merging the physical and the cyberworlds that is now happening. For all these reasons there is a strong case for either the second or the third strategy option outlined above.

On a more general note, the examples of edge computing proposed in 5G and a new QoS paradigm [12] show how precarious it is to write technology dependent regulation. Rather than go there, it would seem wise to focus in banning or restricting harmful business relationships and practises and avoid technical detail to the maximum degree.

The example of Smart Grid security shows how the lack of generic security support on the Internet is likely to lead to some type of *segmentation of the Internet* for supporting the Industrial Internet and more widely digitalization of the economy and all kinds of critical infrastructure. These new needs will not be met by the Internet in the narrow sense but by specialized networks that are built on the same infrastructure as the

Internet but will be isolated from it. Secured remote access to these critical segments can be provided by mobile networks to devices that all will have a SIM card. To attack such segments, the attacker will need to use compute resources that also have a SIM card at a suitable operator and may be even that will not be enough.

Finally, the impact of EU NN onto industry structure is that the regulation greatly favours US cloud companies on the new battle field of virtualised network-based services. All kinds of 5G style and other cloud services by the cloud players are unregulated while European MNO operations are regulated under NN. The outcome is that European MNOs are hampered from re-inventing themselves as cloud services companies where the technology shift is pushing them. It is hard to imagine why EU is doing this kind of disfavour to its own industry.

Bibliography

1. Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union *OJ L 310, 26.11.2015, p. 1–18*
   ELI: http://data.europa.eu/eli/reg/2015/2120/oj
2. Body of European Regulators for Electronic Communications, BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules.
3. J. Scott Marcus, "Network Neutrality Revisited: Challenges and Responses in the EU and in the US", a study on behalf of the European Parliament's IMCO Committee, 2014, IP/A/IMCO/2014-02, PE 518.751.
4. E. Obiodu, N. Sastry, A Raman, Towards a taxonomy of differentiated service classes in the 5G era, 2018, IEEE 5G World Forum (5GWF).
5. Z. Frias, J. Perez Martínez, 5G networks: Will technology and policy collide? Telecommunications Policy 42, September 2018, Elsevier.
6. Tim Wu, Network Neutrality, Broadband Discrimination, Journal of Telecommunications and High Technology Law, Vol. 2, p. 141, 2003
7. M. H. Lofti, S. Sarkar, G. Kesidis, Migration to a Non-Neutral Internet: Economic Modeling and Analysis of Impact, 2016 Annual Conference on Information Science and Systems (CISS).
8. H. Schulzrinne, Network Neutrality Is About Money, not Packets, IEEE Internet Computing, Nov/Dec 2018.
9. P. Maillé, G. Simon, and B. Tuffin, Toward a Net Neutrality Debate that Conforms to the 2010s, IEEE Communications Magazine, March 2016.
10. K. Hartmann, K. Giles, Net Neutrality in the Context of Cyber Warfare, 10th International Conference on Cyber Conflict, 2018, NATO CCD COE Publications, Tallinn.
11. V. Cerf, Internet and Jurisdiction, IEEE Computing, March/April 2018.
12. K. Kilkki, B. Finley, In Search of the Lost QoS, preprint in Cornell University, arXiv: 1901.06867.
13. T. Lohninger, B. Gollatz, C. Hoffmann, E. E. Steinhammer, L. Benedikt Deffaal, A. Al-Awadi, A. Czák, Report "The Net Neutrality Situation in the EU – Evaluation of the First Two Years of Enforcement", epicenter.works, Vienna, 29.01.2019.
14. J. Taplin, Move Fast and Break Things, How Faeebook, Google and Amazon have cornered culture and undermined democracy, ISBN 978-1-5098-4770-9, Pan Books.
15. Cloudstreet, the user defined network, network slicing in practise, white paper, 2017.
16. R. Kantola, J. Llorente Santos, N. Beijar, Policy Based Communications for 5G Mobile with Customer Edge Switching, Wiley Security and Communication Networks, 05/2015; DOI:10.1002/sec.1253.
17. K. Nieminen, Chairman of BEREC working group on NN, e-mail exchange, March, 2019
18. Federal Communications Commission (FCC), 47 CFR Parts 1, 8, and 20 Protecting and Promoting the Open Internet; Final Rule, April 13, 2015.