Bird & Bird LLP
Zuid-Hollandplein 22
2596 AW The Hague
P.O. Box 30311
2500 GH The Hague
Netherlands
Tel +31 (0) 70 353 8800
Fax +31 (0) 70 353 8811
twobirds.com

INTERVIEW

Interviewee: Thomas Lohninger / epicenter.works
Interviewed by: [redacted] / Bird & Bird
Date of interview: 24 July 2018
Our Ref: European Commission, Brussels / EUROC.0020
Re: Transcript of interview with epicenter.works

INTRODUCTION

1. We would like to use extracts or information from the interview in our report, but we won't add the transcript of the interview as an Annex to the report. Is it alright for you if we use this information in the report?

Yes, I am fine with that.

2. It would also then be clear that the input came from epicenter.works if that is okay?

Yes, I am also fine with that.

GENERAL

3. To what is extent is your organisation affected by the net neutrality provisions?

Our organisation cares deeply about net neutrality and the open internet. And as we followed the legislative process from the beginning, and are also very engaged in the enforcement and receive many communications from users, from other NGO's, we have a great overview of the net neutrality enforcement situation. There is almost no net neutrality violations or regulatory case happening in Europe which we are not looking at. We are directly affected, although we are not a CAP or an ISP, but with regard to user interest and consumer interest, we see us as affected.

4. In general, do you think the Regulation works as intended?

Yes.

5. What works well?

I believe that the Regulation itself works really well. The only problem that we have is with the Guidelines and with the implementation of the Guidelines. We see very solid decisions when it comes to the enforcement around traffic management and the prohibition of blocking, throttling or modification of traffic, and also unreasonable prioritisation of traffic. But the big problem is around commercial practices, particularly zero-rating offers. We see wide-spread inaction from NRAs on zero-rating, although we believe that the Regulation is very clear in prohibiting certain harmful commercial practices and even obliges NRAs to intervene, as is laid out in Recital 7. There is a great variation in the extent to which individual commercial practices infringe on end-users rights to use and offer services.

6. You mention all different kinds of zero-rating. What elements are you focusing on, is it traffic exceeding the datacap, or the categories that are being defined? Could you explain that a bit further?

One can infringe the principle of net neutrality technically and commercially. We observe good enforcement against technical discrimination, but we have also seen huge problems in the enforcement against all types of commercial discrimination (price differentiations between applications and services, zero-rating). The Guidelines follow a very soft reading of the Regulation in this regard. The Regulation itself clearly prohibits commercial practices or agreements which restrict end-user rights. To our knowledge not a single regulator has intervened regarding commercial discrimination, not even in extreme cases like in Portugal and Germany where there is a clear decrease of user choice and increase of market entry barriers, given the high price for general data volume in those mobile markets. Zero-rating offerings are now common practice in almost all European countries and regulators have stood by and done nothing.

In part this problem was created by the Guidelines. They postulated in paragraph 48 that such offerings are less infringing when they apply to a whole class of applications or services, in contrast to individual application or services. Many zero-rating offers around Europe have followed this model. We categorise them as "open-class based" zero-rating offers, because they arbitrarily define a class of services (social vs. chat) and offer some more or less elaborate way for CAPs to enter into agreements to participate in that offering. Examples would be StreamOn in Germany, Vodafone Pass in various EU countries, and Smart Net in Portugal from the provider MEO. Such offers really have a detrimental effect on the digital single market. A CAP might be aware of such offers if they are located in the same country and hears about it in the media. But for the majority of European CAPs such agreements create new market entry barriers and hinder their innovation. A provider which would want to compete with companies like Google or Facebook on an equal footing would have to enter into agreements with liability for any wrongfully billed data volume in 31 countries and in 26 languages. Even companies that have experience with such offers like Spotify have failed to adapt their service in time and could only participate in Germany several months after the introduction of one such offer. We see these types of offers as the biggest net neutrality problem in Europe right now.

7. This is a very important element that comes up in many of the surveys and interviews. For example in the Netherlands we have the T-Mobile offering and you also probably know that the Dutch court has given the ruling that the Regulation does not prohibit per se every zero-rated offering. But, of course, which certain guarantees and elements. Did you have a look at that and do you see any differences between that offering and the one in Portugal, for instance? Or the German offering?

Yes, I am aware of that offering and the case you are referring to. The T-Mobile Data Free Music offering is quite similar to the Deutsche Telekom offering, called StreamOn, which is modelled after the US version called BingeOn. You can find similar types of zero-rating offers as a group strategy. The Portuguese regulator ANACOM recently handed down their decision on certain mobile internet offerings. One of these included an explicit restriction of internet access to just a hand-picked selection of services and the sale of specific data volume only for these services, without the technical possibility to use the open internet. The Portuguese offering

was the most extreme case of commercial discrimination that I have ever seen in Europe and in my opinion it is clearly prohibited under the Regulation. Yet, ANACOM only prohibited the technical discrimination aspects, which in effect created sub-internet offerings. The commercial discrimination aspects were allowed to continue. The proceedings and the final decision were made only in 2018 after the offer could exist for several years since the Regulation came into effect, and only after there was an intense public debate and public pressure by consumers that sought protection. The decision was consulted by ANACOM. The response that our organisation gave together with several other digital rights organisations showcased the shortcomings of these products. We are talking about a situation where the three biggest mobile operators with a total of 95% market share in Portugal are involved. All zero-rated Facebook, Youtube, and several other big Silicon Valley companies. The only other domestic OTTs that were zero-rated were in-house services of those ISPs and you could almost find no other OTTs from other European countries. This is an architectural shortcoming of all these open class-based zero-rating offerings, like T-Mobile NL Data Free music, StreamOn, A1 Free Stream or Vodafone Pass. You can basically split all OTTs in these offerings into either domestic or Silicon Valley companies. Very rarely do you see any offerings or OTTs from other European Member States, which adds to the already strong national segmentation of the digital single market. And sadly, this is the outcome of the scope of the current review of the NRAs, and as we pointed out repeatedly, these questions have not made their way to the work programme of BEREC. A comparative analysis of such commercial practices and agreements is a big blind spot, which should also be pointed out to the Commission, because the interdependencies in the national enforcement of the Regulation created a situation which is particularly harmful for the availability of online services across European Member States.

8. Does the Regulation sufficiently protect fundamental rights, such as the freedom of expression, the right to privacy, etc?

Regarding fundamental rights, there is now a big problem that we see in the technical design of these products. This is true for T-Mobile Netherlands' Data Free music, as well as almost all of these open class-based zero-rating offers that, in theory at least, allow OTTs to join these programs. They all offer identification criteria for those services which operate on the innermist layer of the internet information architecture. For example, Deutsche Telekom allows URL or SNI identification as attributes for OTTs to help the operators to identify the traffic of their services in order to make it zero-rated. These attributes are on the application layer, the innermost layer of the internet architecture (OSI model), which means they should normally not be looked at or touched by ISPs. According to Article 3(4) of the Regulation and also the definitions regarding specific content in the Guidelines, these attributes have to be seen as specific content, and they of course contain user information, like the specific resources users access on servers with which they connect. The fact that these attributes, which are clearly protected under the GDPR and the ePrivacy Directive, and also under the Regulation, are utilised for the creation of such products is a big problem that, sadly, NRAs do not feel responsible for. This data protection aspect is another great shortcoming in the design of these products. To my knowledge, very few operators are already asking for consent to the processing of this personal information from their own customers, let alone have other users and providers on the internet that connect to or are connected by their customers consent to the processing of this data. I would also argue that such a level of control and such a fine level of distinction on the billing

also undermines the goal of the Regulation, because it puts far more control in the hands of internet service providers than any previous business model in the internet has done.

9. Is that also related to the use of IP-addresses in the zero-rating offerings?

IP addresses are on an outer layer of the internet architecture and are therefore, in the context of these particular commercial practices, less problematic. If all services could be sufficiently identified by IP addresses that would mitigate the privacy problem I was just talking about. To be clear, a large number of European citizens are now using internet access products that require deep packet inspection technology for their business case. And that is a problem that regulators should pay more attention to. Again, it is sufficiently clear in the Regulation and other European legislation how these things should be treated but there is no interest of the relevant telecom or data protection regulatory authorities to properly do enforcement around these products, and there is not enough guidance on this category of open class-based zero-rating offers from the BEREC Guidelines.

10. So, your main concern is actually that there is a difficulty in the enforcement. A delay or abstaining in the enforcement action and therefore these practices can continue, and that also causes a difference in Member States?

Yes, one could summarise the current situation around enforcement as no regulatory authority wants to be the prime mover on zero-rating. Particularly because they expect to be sued, with almost everything they do, and such court cases are looming over them, creating situations in which only the most conservative rulings are issued. This situation is to the detriment of users' rights. Particularly in light of Recital 7, which clearly obliges regulators to intervene in certain cases, such inaction has to be seen as a shortcoming of enforcement.

And finally, I would also wish to stress that there is very poor data on the factual situation regarding the differences in zero-rating offers. For example, there is no scrutiny of the sign up procedures for CAPs that ISPs have integrated into these open class-based zero-rating products. In Portugal, in the case of "Smart Net" from the incumbent operator MEO, weeks before the regulator had announced its decision, an email address to participate in the previously closed zero-rating program was published in the fine print of the offer. To our knowledge none of the CAPs which tried to apply to this service ever got a response. Yet, the regulator argues that there is no damage done to competition because the product offers a sign-up procedure. If regulators would look closer, they would see that products like T-Mobile's Data Free music and other open class-based zero-rating offerings are actually discriminatory and favour established CAPs.

We have provided data along those lines in our previous submissions which can be found in the documents section of our website (https://epicenter.works/documents?field_tags_tid=4).

11. To make sure we understand you correctly, the position is not that every and all zero-rating offerings are a violation of the Regulation, but there is still an element of discrimination in the offerings that are currently applied across the European Union?

So, I would argue that the Regulation is very clear in prohibiting of a specific form of application-specific zero-rating or application-specific data volumes. Any commercial practices or agreements which are to the detriment of end users' choice and which go against the requirement under Article 3(3) of equal treatment of traffic would, in my opinion, be illegal under the Regulation. We also see that the case-by-case approach on zero-rating offerings mandated by the BEREC Guidelines is not working, simply because it has never been properly applied, not even in the most extreme cases.

12. The NRAs have the possibility to do joint research, joint investigations, for example to resolve the lack of data on cross-border traffic. Is it then the problem that they do not use the powers that they have?

As we stated in our response to the consultation of the BEREC work programme, yes, they have the possibility to conduct such research, but to my knowledge it has not been used in this field. But I think that is an area where the Commission could also conduct a study. The Commission already publishes a very useful data set on mobile broadband prices. Particularly considering the argument of some telecom operators that consumer choice mitigates all effects of commercial discrimination, it would only be logical to also publish information about each zero-rating offer in Europe and the participating CAPs. It would be a highly informative data set to all parties involved.

13. Does your organisation spend more resources as a result of the implementation of the Regulation?

Yes, we are very involved in the enforcement in most EU member states. We are a small team with a small budget, funded only by donations and grants, but we believe it is important to have a civil society entity that tries to keep up with all cases and proceedings surrounding net neutrality in Europe and draw conclusions for the global debate.

14. What would you say that you would spend most resources on? Zero-rating?

I will try to summarise. We are focussing on end-user rights and zero-rating. We are also working on traffic management. We are advising BEREC and other NRAs on their monitoring mechanisms. We have been researching port blocking and blocking and throttling of content.

By the way, there are shortcomings in the amount of detail when it comes to port blocking in the annual reports that NRAs have to issue. So we actually wish for a bit more harmonisation in the way in which traffic management measures have to be made transparent in the contract according to the obligations the Regulation stipulates in Article 4(1). But also in the way the regulators summarise these port blockings or other traffic management measures in their annual report.

I have already talked about the implications of the processing of personal data when it comes to commercial practices and agreements. We are always looking for interesting news on specialised services. One particular point I would like to stress is that we have also looked into Member States' penalty provisions according to Article 6, and you can find on our website (https://epicenter.works/document/1255) an open letter, and complete data set on penalty provisions for net neutrality violations that Member States have imposed in national legislation. The lowest maximum fine for net neutrality violation is EUR 9600,- in Estonia and the most highest is in the UK with 10% of the annual turnover. I would argue that the requirements of Article 6 are not fulfilled by the majority of Member States.

15. Has your organisation been in contact with any of the following NRAs, ISPs, CAPs, COs, CPAs, etc?

Yes, NRAs, ISPs, CAPs, consumer organisations, consumer protection authorities. Also with data protection authorities and with the European Commission. We are also talking to the media.

16. Which particular stakeholders have you been in contact with?

I would like the record to reflect that I cannot give you this information in light of the conflict of interest that I see. Bird & Bird is actively involved in litigation on the enforcement of the Regulation, therefore I would like to not give you information about which explicit stakeholders/topics we are in contact with.

17. That is fine. Just to make it clear, what we are doing is based on the mere facts. There is no policy element involved, just the inventarisation on the basis as-it-is. What topics were mainly discussed with the different stakeholders?

The main topics we are discussing are zero-rating, data protection and specialised services. But also monitoring, very important now is that the BEREC measurement tool process is already underway. This issue has been most prominent in our recent communication.

18. Do you notice any differences between Member States where stakeholders are very active or less active?

Not that much, of course there are regulators that have more or fewer resources. This is a determining factor, but the issues are more or less the same everywhere.

19. How do most cases or issues reach you? Is this through complains, own research or other channels?

I would say mostly through our own monitoring. We are looking at what regulators are doing, how the market is behaving, and of course, many are brought to us by people on the ground, like consumers, CAPs, or from local NGOs.

ARTICLE 3

20. Article 3(1) - Do you think the wording in the Regulation is sufficiently clear when it comes to the end-user's right to access and distribute information and content, use and provide applications and services?

I believe that the wording of the Regulation is very clear on that point. However, I believe that we have a problem with the implementation, but that stems from the Guidelines and not from the Regulation itself.

21. Do you think the implementation through the Guidelines is not in line with this? Has this also led to diverging implementation or NRA behaviour in different Member States?

I do not believe that we have a divergent enforcement on that question. I believe that it stems from the Guidelines and those should be fixed, but because the regulators have to give the utmost account to the Guidelines, this is not a problem that arises from individual Member States, but from the Guidelines themselves.

22. On what elements do you consider the implementation in the Guidelines not to be in accordance with the Regulation?

I believe that we can find clearer guidelines in the Regulation about which form of commercial practices and agreements are prohibited and require regulatory intervention. Explicitly, application-specific forms of such practices. Sadly, the Guidelines only set out a minimum baseline of how regulators could assess certain cases, but the Guidelines don't contain the cases under which the regulator would have to intervene. Although such cases are clearly foreseen by the legislator in the Regulation, the Guidelines have blind spots on that. This is something BEREC should focus on in any potential review of the Guidelines. Right now, if you look through the provisions that are handed down, based on Article 3(1), or 3(2) or also 3(3), when it comes to zero-rating, not even the decisions that regulators come to are actually that stringently argued around the case-by-case assessment that was outlined by the Guidelines.

23. Article 3(2) - The prohibition to limit open-internet access, which also includes zero-rating. Do you think the wording in the Regulation on zero-rating is sufficiently clear?

Yes, I believe so. There is no problem with the Regulation on that front, the problem stems from the Guidelines.

24. Could you elaborate on the different issues that arise from zero-rating?

Yes, the biggest problem is really the detrimental effect that zero-rating has on the availability and portability of individual applications. And also the innovation capacity of the internet. Because there is a huge discrepancy between the amount of resources that are required to provision an online service in an internet that treats all packets equally, both on a technical as well as the commercial level, and any other system where, via agreements and commercial practices, distinctions are made between those services. Such systems ultimately, particularly from a European digital single market perspective, have negative effects. I think we have to

look closer at those negative effects and conduct more economic analysis on that front.

We have for example conducted economic analysis on the impact of zero-rating offerings on the price level of data offerings. If you look up our submission to the Portuguese case (https://epicenter.works/document/1111), we found that there was a large discrepancy between countries where there is no zero-rating, where in general, prices for mobile data volume were falling, and those countries where there is zero-rating and prices for mobile data volume were rising. We could see an over 10% gap between the two categories of countries. I think more such research is required to provide incentive to regulators on that front, because again, it is not a question of the Regulation, ultimately it is about understanding the effect of such commercial practices. Most Regulators are saying that they are not ultimately deciding whether a certain commercial agreement is line with the Regulation. The only thing we have heard from them is, 'so far, we have not seen anything wrong'. And that means they are leaving the door at least a little bit open to revisit these issues. And we believe they should.

25. What was your finding again about the price?

In countries without zero-rating, prices are falling. In countries where there is zero-rating or zero-rating is newly introduced, prices are rising, which should not be the case in the modern day and age. We are comparing the price per gigabyte, and as technology is upgraded to provide for larger network capacity, prices should fall. Our analysis is based on the data that the Commission has published on mobile broadband prices. We found that zero-rating has a negative effect on the affordability of internet access service in general. And that is not even the level that we should look at. We should look at the prices of individual applications that a user wants to use or an OTT wants to offer. This is just looking at the plain and simple national price levels of mobile data offerings in the individual countries and doing a regression analysis on the impact of the availability of zero-rating offerings.

26. Is there anything else that would you like to add, apart from zero-rating, in relation in Article 3(2)?

In relation to interview question 3.3.2.6 ("If you could make any recommendations regarding the Regulation and assessment of zero-rating, which would those be?") *I would seriously consider also understanding these commercial practices, like zero-rating or application specific data volumes (like we see in Portugal with "Smart Net") as a treatment of traffic. Because, technically, what is happening, in order to count data packages differently depending on which services is used, you have to aggregate a certain amount of data packages to even unpack the next layer of information. Technically and physically there is a treatment of traffic happening. This can even be measured in certain cases, depending on the deep package inspection equipment that is utilised by the ISP. More enforcement and also regulatory scrutiny on the way these commercial practices are typically implemented in the core infrastructure of the ISP would also be a very insightful way for regulators to better understand how these products are actually provisioned. But I see no problem with the Regulation yet, as those questions could be easily answered under Article 5, supervision.*

27. About traffic management, Article 3(3) – Do you think the wording of the Regulation is sufficiently clear?

So I think it is sufficiently clear what types of traffic management measures are allowed and I am also not aware of any discrepancies between Member States where it comes to the enforcement of the restrictions of traffic management. In general, I see the biggest problem when it comes to traffic management in the throttling of adaptive bitrate video traffic. Because – to my knowledge – this is something that is not equally applied in every country, for example in certain Vodafone Pass offers the throttling of adaptive bitrate video traffic is only applied to participating OTTs. In other zero-rating offers, for example from T-Mobile, it is applied to all adaptive bitrate video-traffic. You can see a discrepancy here between the strategies that ISPs have chosen to design their products according to the Regulation. There is actually only very weak reasoning behind the supposed legality of the intentional deterioration of service quality which follows a commercial intent, namely to limit the amount of zero-rated data volume passing throught the network. Basically to not zero-rate HD video traffic, but only deliver DVD quality of these same videos when they are zero-rated in order to save network resources. I think this is something where we have an unharmonised approach from the regulators, and maybe that is also where the Guidelines should be a little bit clearer. The general question is whether the ISP optimises for the quality of the service or the resources of its network. The Regulation is clear that the latter is no justification, because if an ISP could make individual services intentionally be delivered in a poorer quality in order to save network resources, the whole architecture of Article 3(3) would fall apart. If Article 3(3) could be circumvented by commercial practices according to Article 3(2) (which only references Article 3(1)) there would be no reason why Article 3(3) subpar 2 should mention "commercial considerations". The whole logic of certain ISPs is flawed in these cases.

28. Article 3(3) – Is throttling is the main traffic management measure that you encounter?

Yes. But we hope to gather more information once the BEREC measurement tool is operational.

29. We would like to hear your views on the blocking of ports, because from our research there comes quite a diverse picture (which ports are blocked in which countries, for what reason and whether that is a problem or not).

We do not hold an ultimate opinion on this issue, because this is something that is evolving, and it also has to be seen in context. To give you an example, I think it was Finland, the Finnish regulator, who gave guidance to the ISPs regarding certain ports they recommend to be blocked. The reason for this actually quite extreme measure was that Finland was seen as a spammy country with many autonomous systems and Finnish ISPs were actually on Spam blacklists, because so much bad traffic was coming from them. That is why they chose to have this measure to block certain e-mail and security related ports to improve the rating of their country when it comes to spam. That is why it needs to be seen in context. It is also something where outside factors would need to be taken into consideration, when we talk about which actual remedies regulators would utilise. I believe that the Regulation offers them enough flexibility.

One issue we have experienced as problematic, ISPs try to mitigate security problems in their routers not by securing the device and patching it so it is no longer vulnerable, but by taking the measure of blocking the port via which a certain attack reaches the customer premise equipment. Such a port blocking in case of an immediate attack is of course justified, but it cannot be, or should not be seen as a legitimate form of long-term mitigation. This is something where we had cases in Germany, where this method of port-blocking was utilised in a permanent way. That is neither to the benefit of the network, because the more ports are blocked, the more unpredictable a network behaves, and also not to the benefit of the security of the users, because the problems need to be fixed by removing the vulnerability, not in fighting individual attack vectors.

It is very important to read the Regulation carefully when it comes to security exceptions and also exceptional traffic management measures in general, because such exceptional measures can and should only be applied when and for as long as necessary. Therefore, we should never consider it a permanent fix, but once regulators take that into account – and, again, we would ask for more transparency on the enforcement of the restriction of traffic management measures – we believe those problems can be solved within the current framework.

30. This is more or less a technical question, but do you have some background information why specific ports are so likely targets for attacks? Looking at Finland you see that there is the obligation to block port 25 altogether, but there is also 53, 123, 1900, 7547. Do you know where that comes from?

There are basically two reasons why port-blocking is utilised. The first one is spam, where providers try to prevent their users or the viruses on the PC's of the users to send out useless spam emails that are also bad for the rating of their network. Networks are rated according the amount of spam that comes from them.

The second reason is security measures. Computers with insecurely configured or unupgraded systems, or IoT devices without security upgrades can become easy targets for an attacker. The blocking of port 123 is likely such a case. Certain ports are particularly well known for exposing attack surface to the wider internet. Some of them would also be more typically used within a local network and usually don't get exposed to the internet, because you don't want a third party to connect to services running on that port. This is the case with port 1900, which is typically used for a service by which customers can control their customer premise equipment from their local network. Port 7547 is typically used for remote management of customer premise equipment by ISPs, this is probably an example of a security measure mentioned in the answer to the previous question. The blocking of port 53 could be a security measure, but might also be part of a measure to censor access to certain sites.

31. FICORA list is the most extensive list that we are aware of. Do you have an idea or a view about the extent of port-blocking throughout the Member States? And whether for instance port 25 is blocked almost everywhere?

We do not have such overall knowledge. We have been criticising some NRAs about the lack of information on this issue in their annual reports. We are also missing this summary in the BEREC report. But I believe that the Regulation is good and gives the flexibility to take care of the national circumstances.

The real problem is that regulators are hesitant to be too specific about such a hot potato and it's so easy to get those things wrong, that it's often a more comfortable situation for regulators to let ISPs deal with it. The problem is that users are again often caught in the middle and that's why, besides the annual reports of NRAs and BEREC, also the information that ISPs publish about port blocking and other traffic management measures is often insufficient. The utilisation of the network would need to be far more up to date and detailed and should really give users the ability to make informed choices. This is really something where transparency would be sufficient to solve the problem in terms of the Open Internet Regulation. I can't speak to the perspective from the NIS Directive.

32. Article 3(4) processing of personal data - We already discussed this in the beginning with regards to Deep Packet Inspection. Is there anything that you would like to bring forward here?

I think we more or less covered it. I would wish for more regulatory scrutiny and also we are thinking about this issue, how to actually get more of these commercial practices in line regarding to the data protection framework.

33. Could you maybe go back once to your point and your concerns in relation to Deep Packet Inspection?

To give you one example. If you're unhappy with your bill, consumer protection law allows you to file an objection, and the provider has to store your communication metadata on the calls that you have made and the SMS text messages that you have sent, so that you could on a factual basis assess whether this bill is correct. The calls and SMS are billing data. In the products that we are talking about, and it includes several of the zero-rating offers, the URLs the customer accesses in fact become billing data because they have a direct impact on the amount of data volume that they have to pay for. This is again one of the issues where I believe more regulatory scrutiny would be necessary and where again I believe that current commercial practices and agreements have not been fully understood.

34. But then the main concern here is that there is personal data that are not appreciated as such and not qualified as such. And therefore are falling outside the scope of Article 3(4) and also the data protection Regulation.

Exactly, so it is not understood that in fact an URL contains a lot of information on my communications behaviour. For example, there is the content of all of the Google Translate requests that I'm sending. It contains a lot of personal information and it is processed by the ISP. That also includes information from third party users that connect to a user of such a zero-rating offer and they have not consented to these types of processing of their data.

35. Article 3(5) – specialised services. Do you think the difference between IAS and specialised services is clear for all stakeholders based on the wording of the Regulation?

We also couldn't find good examples whilst we were discussing this Regulation with the Commission, in the Parliament, in the Counsel, etc. You can find in the public records that we've been asking many times for specific examples of specialised services. We've been questioning why we are creating a particular legal basis for a type of access service which circumvents net neutrality protections. Nothing was

preventing ISPs from provisioning specialised services before the Regulation was adopted. Yet, we have seen no successful examples of such services in the decades since the internet was created. Without net neutrality there was absolutely nothing stopping ISPs from creating whatever type of access service they want. The Regulation therefore rightfully puts an emphasis on open internet and the type of access services which have created huge economic benefit for society, like we have never seen before. At the same time the Regulation as well as the Guidelines are opening up the possibility of specialised services wherever they are not to the detriment of the open internet.

I believe that with 5G business models we might actually see more experiments of ISPs with specialised services. But the current Regulation and the Guidelines are both capable of dealing with those issues. There are good reasons why laws are written in language which is technology neutral. It would be a shortsighted political decision to lower protections of one of the most promising branches of the economy in order to enable questionable business models which have neither materialised nor demonstrated how they would benefit us. I would also point to great studies that have come out recently that basically say: "The only thing that is certain about 5G is that we'll get faster internet". There isn't anything in there that would indicate an incompatibility between this new mobile technology and the current regulatory framework (see https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8008-study-on-implications-of-5g-deployment-on-future-business-models).

Therefore, we are happy with the current text and we are all looking forward to the findings of the BEREC consultation in which they have also asked about concrete examples of specialised services in 5G and certain possible incompatibilities between the Regulation and those new access services and business models. I hope that those findings can clarify the question that we have all been asking since the beginning of what exactly those specialised services should be. We don't believe that it is health services because those are already there. And all the other examples. If autonomous cars needed a constant network connection in order to function, they are not autonomous cars, they are remote controlled cars that could never pass a tunnel or a mountain village. I also can't imagine medical surgery that is anywhere close to a critical condition which could ever use the same infrastructure as the internet. You'd want to have dedicated lines and a physically separated connection, in order to ensure the required amount of quality and stability. These types of things surely cannot be achieved by the same internet infrastructure which always incorporates too many autonomous systems that behave differently. Also, specialised services over that same infrastructure would not be able to achieve this. Therefore, we believe we are in a very good position on the question of specialised services because all truly novel services can be provisioned. Nothing is stopping telecom providers from being innovative in that field. At the same time, since the beginning we've been warning that specialised services should not be abused to circumvent net neutrality. Existing online services should not be allowed to be re-classified as specialised services. But we believe that the Guidelines and the Regulation are both very clear on these questions. We should not change rules that have worked so far in order to accommodate promises of unsubstantiated business models.

36. Do you notice a difference in the attitude of NRAs or other stakeholders towards specialised services?

No, not really. I also haven't come across this.

37. We are only aware of one enforcement case in the EU regarding specialised services and that is in Austria. Can you give your views on that specific case?

It's a kind of curious case. The Austrian NRA has made the right decision here. The behaviour was incompatible with the principle of net neutrality and the letter of the law.

38. It would be helpful to have a bit more background.

I'm sorry I cannot go into detail.

ARTICLE 4

39. Article 4 – To what extent is this Article relevant for your organisation?

I think Article 4(1) is an underrated Article and we wish that more regulators would actually use the possibility that they have to lay down rules on how specifically the information of 4(1) has to be provided. Having comparable datasets on how internet access products differ would be a powerful tool for consumers to make more informed and better choices. Right now, at least in the contracts that we have analysed, and of course this is in no way representative because we don't have that many resources, we see that there is a huge discrepancy in the amount of information that is actually provided by ISPs. I believe also that there are other infrastructures that would be required for aggregating this information on independent platforms that allows consumers to really see the differences in a one-stop-shop-principle and not inquire 20 ISPs for their contracts and then compare it manually.

So this is a good Article, but it would require more regulatory scrutiny and it is something that maybe BEREC should also give more guidance on. The Regulation is sound here, the problem would be that too few people are actually looking at this. Article 4(1) gives you enough information to allow for more informed and better choices, we are not just there yet.

40. In your experience do you see NRAs actively enforcing the contract information requirements?

The only case that we ever had on transparency concerning zero-rating in Europe was an Article 4(1) violation in Belgium. So that was not the zero-rating offer itself that was prohibited, but it was that the product was not transparent on the effect of data volume, and therefore the Belgian NRA issued a penalty and asked the ISP to be more transparent about that. There are possibilities for regulators to lay down further rules on how this information actually has to be published. This should be utilised more. The Article does not have to be changed.

41. Article 4(2) - In relation to end-users complaints, to what extent are you aware of NRAs having supervised and enforced the requirements that ISPs must put in place on procedures to address complaints from end-users?

I'm not aware of any such activities. To my knowledge most NRAs have not even published information on how users can submit complaints with them. The numbers

of received complaints varies greatly between NRAs and according to the 2017 BEREC net neutrality enforcement report only six NRAs have specifically said they updated their websites (page 5).

42. Do you see any complaint procedure in a Member State that works well?

I think the French regulatory authority ARCEP has introduced a complaint mechanism via which users can actually enter into a formal proceedings and also receive more information about the complaint while it's being processed. I was pointed towards that as a possible guidance on how it should be done.

43. Article 4(3) - We already discussed the possibility of additional requirements, which are too little for your opinion, correct?

Yes.

44. Article 4(4) - Certified monitoring systems: To what extent do you believe that you can benefit from a NRA certified monitoring system?

We believe that this is an integral part of the Regulation and this is really something where the interest of regulators to have as few cases as possible, the interest of users to have a good understanding of the internet access products they are actually buying and the interest of any government to have a good data set about the internet infrastructure all align quite neatly. We strongly supported the BEREC measurement tool development and gave them guidance in consultations at various points. This is a positive step forwards. We hope this certified monitoring system and the incorporated open data pool of measurement data actually creates a cloud of data points which increases the risks for ISPs that unreasonable traffic management practices are detected by independent researches or NRAs. For example, if I'm an ISP and I want to engage in unreasonable traffic management measures, but I know that there are thousands of internet users that use a certified measurement software which can detect a wide variety of traffic management measures and creates an open data record of my potential misbehaviour, I would think twice before doing anything outside the regulatory boundaries. It is not just a tool for transparency, it is also a tool for enforcement and supervision. I believe that Europe can really lead on that role (the Indian regulator is looking at what Europe is doing). This BEREC tool is a great contribution to measuring the internet and it would be a great step forward if we could set a global standard here.

One thing to add is that we should aim for a unified measurement tool in Europe; having 28 measurements tools is not an efficient use of resources nor does it help us to create comparability of results. Also in terms of visibility a European wide solution is preferable to 28 national ones.

45. Do you have any insights as to why NRAs decided not to come to a harmonised approach, so far?

Path dependency. Every NRA that already invested in their own tool is proud about what they have done, they believe they are the bravest and brightest, they found the ultimate solution and they spent money on it. I don't believe that any particular tool has set the golden standard: all of them have good and bad aspects. We should really try to combine the best of them and create a uniform solution, particularly if we aim for an open source, open data approach it would be good if all sources are

bundled. There are no good reasons in my opinion why we should not aim for a harmonised system. But I believe that this question is solved now that BEREC approached it. We are on a good path.

46. Do you believe that online tools lower barriers for consumers to successfully raise non-conformity of performance claims?

Yes, such tools have to be pragmatic and they have to be where people use the internet. I am strongly in favour of using apps or website based tools, instead of taking hardware measurements, because those are just not as accessible to people. Everybody uses a smartphone, everybody uses a browser, but requiring hardware based measurements excludes many people, doesn't capture user experience and is more expensive. In the call for tenders, BEREC has chosen the right approach to actually ask for online tools.

ARTICLE 5

47. Article 5(1) - Do you see different approaches on supervision and enforcement in different Member States and/or a difference in the level of activity of the NRA?

Yes, I believe that in general the bigger the country is, the more politically loaded the situation is for the regulator. Because in the bigger countries the government still holds shares in the former incumbent and the bigger the telecom operator the more likely they are to violate the principle of net neutrality, just because it makes more economic sense to monetise scarcity if you are the biggest kid in the school yard, if you have the largest customer base. Those are the two factors which contribute towards a certain misbehaviour of companies which are softer regulated by their NRA, because they are part of the government (although on paper they are independent). Therefore, it is hard for NRAs to issue a decision that would go against these types of behaviours. They would either be very slow to act and if they act they would also try to be as soft as possible. That means to only do the basic necessity of bringing products in line with the basic notion of the Regulation, but not really the letter of the law. For example, the German NRA waited for several months before they issued the decision against illegal traffic management practices of Deutsche Telekom as part of their StreamOn product. The company throttled adaptive bitrate video services in certain contracts and only combined fixed and mobile (hybrid) customers were exempt from this throttling. The first report of Deutsche Telekom for Q1 2018 shows that the only significant growth in Germany is in the hybrid customer segment with +16%. When the decision of the regulator was finally issued 9 months after the product was launched, the penalty for Deutsche Telekom was only EUR 100.000,- out of the maximum penalty of EUR 500.000,-. The Austrian NRA issued a similar decision against Telekom Austria within only one month. Here you see big problems.

This is not just true for big countries, because if you look at for example Vodafone Pass, which was started in almost all countries that Vodafone is present in, every regulator waited until Ofcom in Great Britain issued their decision and then more or less followed that line. If you look at the history of the Open Internet Regulation, the Commission originally proposed a system where any multinational telecom operator would only be regulated by the NRA of their home country. This actually seems to be the case now, although this system was deleted by the Parliament and the Council. Most regulators wait until the country where the mother company is

situated has issued a decision. That of course kind of exports this unwillingness to go against these multi-national telecom companies to all European countries to the detriment of smaller operators and to the detriment of competition.

48. Would you recommend a more uniform and harmonised supervision and enforcement approach?

No, we have recently adopted a BEREC Regulation which was a clear political statement against such an approach and I would be opposed to try to open up the same question in the net neutrality Regulation.

49. Which NRA do you consider to be most active in enforcing the Regulation?

I really could not say. I think there are always black and white sheep.

50. Do you see differences in the provided guidance by NRAs? Or is that also quite difficult to say?

This would be something where I wish the BEREC enforcement report would give more summarised information. I cannot answer that question properly from a European perspective.

51. Article 5(2) - To what extent did or will NRAs impose requirements concerning technical characteristics, minimal quality of service and other appropriate and necessary measures in your opinion?

To my knowledge NRAs have not imposed such minimal quality of service requirements, but I believe they should. I believe that there are circumstances under which these powers under Article 5 should be used to establish a certain minimum requirements of what broadband access actually means. I am talking about Germany in that case, where I believe we see great market failure and great problem that at least a basic minimum requirement would be really helpful in order to get people into the 21st century.

52. The BEREC Guidelines. We discussed these already quite a bit. Is it your perception that the NRAs follow these Guidelines?

Generally speaking, yes. I think they give the utmost account to the Guidelines. Where the Guidelines are weak, on zero-rating, we see that the structure of the decisions that are handed down is not entirely in line with what the Guidelines or the Regulation states. However, in general, particularly where the Guidelines are clear, they have exactly the intended effect of creating harmonised enforcement.

ARTICLE 6

53. To what extent do you believe that NRAs apply different penalties in similar cases and that harmonisation is necessary?

I believe that the only action required is from the Commission to actually be more upfront on the long overdue enforcement of Article 6. The deadline was April 2016 (we are more than 2 years after that). We are told Austria is in the process of adopting a telecommunications law. Ireland and Portugal still have not laid down

penalties. As we've outlined in our recent mapping of all national penalty provisions and to a letter to the Commission there is a great discrepancy between the applicable penalties, in some cases it is very cheap to violate the Regulation. We also see a big problem with the fact that some Member States have for some astonishing reason chosen not to establish penalties for all of the Articles of the Regulation. Germany had not laid down penalties on zero-rating, because they don't believe the rules to be clear enough and that is strange because the Regulation is very specific on member states obligations on this question. There is definitely a lack of political will from both Member States and the European Commission to actually uphold the law.

In principle I believe that strong penalties that fulfil the requirements of proportionality and effectiveness should be calculated as a percentage of the annual turnover. That would equally distribute the burden to small and big companies instead of any fixed amount of a maximum penalty which always disfavours smaller operators and gives benefit to big operators that have deep pockets. Big ISPs also give access to services to the most users and therefore should be measured against a higher standard. If you look at any other area of ex-post regulation you'll find this as a common practice. We also don't see a reason why there should not be a clear guidance from the Commission on that question.

I believe that Article 6 itself is set up to the task and does not require any amendment. If the Commission were a bit more upfront about calling Member States to live up to their Treaty obligations in this case, we could actually put this issue to rest.

54. Thank you for the interview.