Joint response of ARTICLE 19 and epicenter.works to Call for inputs on views on the impact of 5G on regulation, and to the role of regulation in enabling the 5G ecosystem

Priorities identified by the Working Group

We welcome the possibility to provide inputs on the potential regulatory aspects of 5G that could merit from further investigation by BEREC. Nevertheless, we reiterate our previous calls for adequate time to answer a BEREC consultation, and remind BEREC that the present call for inputs was launched during the holiday month of August, with an expected duration of four weeks and with a last answering date following only shortly after usual holiday periods end in most EU countries.

We also wish to point out that the Working Group is needlessly restrictive in its survey of available reference materials. We would like to see a more inclusive approach from BEREC, where civil society organizations (representing consumer and digital rights interests, for instance) and businesses are also considered valuable sources for information in, for example, privacy and security topics. Currently, it appears that BEREC aims to consider consumer inputs only in relation to coverage (in *Focus: End-User Perspective* Priority 6).

We wish to make the following observations on the proposed priorities identified by the Working Group in its Call of Inputs:

1. Privacy:

We believe BEREC is uniquely positioned in the EU supervisory landscape to follow up and explore technical standardization, for instance in the field of data portability.[1] However, such work needs to be part of a common approach with the European Data Protection Board (EDPB). We suggest that the competencies referred in Recital 66 of

1 For instance, https://datatransferproject.dev.

Directive 2009/136/EC should be explored, in this regard, to enhance the abilities of BEREC and EDPB to benefit from already ongoing private sector initiatives in standardization, API development and other technical features. See also our observations on security below.

2. Security:

We strongly prefer the broad take on security proposed by BEREC for its *Focus: Verticals perspective* Priority 8, which acknowledges the different requirements or different society actors and how they may come in conflict with one other.

Currently, the European Commission is advancing data protection by design and a "human-centric internet", while network equipment vendors are openly calling attention to how they are being blocked by member state public authorities from introducing necessary and long-delayed security enhancements to end-user communications.[2] Member state authorities are calling for mandatory sharing of encryption keys between networks even in the absence of an activated lawful intercept function,[3] and using their positions in standards organizations to call for the development of data maximization business models, in direct contradiction with European law (Articles 5 and 25 of General Data Protection Regulation[4], or GDPR).[5]

These actions are blocking mobile network operators and equipment manufacturers from advancing security and privacy for end-consumers and European companies, and leaving an otherwise competitive industry falling behind the stronger security and privacy developments advanced by OTTs and similar services.

The regretful lack of coordination between the European level and the member state level, and across different parts of the public sector, risks damaging citizens' trust in their communications providers, their companies and in the European Union. It also damages the ability of network equipment manufacturers to contribute to the realization of European norms and values.

European companies are, in fact, uniquely disadvantaged in the world as being stuck between two different layers of regulatory values: on the one hand, a European layer

2 S. Holtmanns, Nokia Bell Labs. Presentation at ETSI Security Week 2018.

3 3GPP-SA3-LI, Tdoc S3i190258: "*CSP provided cryptographic parameters in roaming – When a home CSP's subscriber is roaming, independently of whether or not the subscriber is an LI Target in the VPLMN, the home CSP shall provide to the visited CSP the means to decrypt user services which are encrypted between the ME and an entity outside the visited CSP and using cryptographic parameters established in the home CSP.*"

4 Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 04.05.2016.

5 Verbal made by 3GPP-SA3-LI chair person in front of the 3GPP-SA2 working group on network architecture in Sapporo, Japan, June 2019. Written recording of the exchange beyond ARTICLE19's reporting is missing.

of values which focusses on trustworthy technologies, security and privacy for the end-user and human-centrism, and on the other, a member state layer of values which focusses on geopolitical competition and national industrial policy and the threats posed by some citizens to national security and to public order.

We remind BEREC, in this regard, of its statutory tasks in Article 3.2.d, European Electronic Communications Code[6], in particular BEREC's and its constituent bodies' obligation to "*promote the interests of the citizens of the Union, by /…/ maintaining the security of networks and services [and] by ensuring a high and common level of protection for end-users*". We propose to include in the scope of future investigations a thorough mapping of legal bases invoked by member state's authorities to justify limitations of security or privacy features in 5G. We also propose that BEREC actively monitors whether adequate legal bases exist for proposals advanced by governments that actively participate in 3GPP standardization activities.[7] Some of the security-reducing proposals advanced, such as encryption key sharing or prohibition of mobile communications end-to-end encryption, are advanced by European public authorities that wish to pre-empt the risk of having to cooperate with other European public authorities.[8] It is unclear to us at this time which EU or national laws encourage or legally provide for the evasion of inter-European cooperation by reduction of security in mobile networks.

Currently, security and privacy mechanisms are being developed in both the mobile network equipment and wireless local area network communities, with regulatory and economic barriers to deployment being the primary stopping block for stronger cybersecurity for all. We suggest that the current lack of credible metrics is creating a scenario where individuals, governments and companies are exposed to greater threats than necessary. For example, if encrypting an IMSI number increases latency by 0.1 millisecond, an operator which is only exposed to latency metrics will sacrifice the more robust security arising from encrypted IMSI numbers. Similarly, if an operator feels obliged to refrain from providing end-to-end encryption to consumer communications, users will ultimately suffer from exposed and insecure communications.

BEREC should consider requesting, in the context of national licensing practices, that

6 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), PE/52/2018/REV/1 *OJ L 321, 17.12.2018, p. 36–214.*

7 3GPP portal meeting records indicate that the following European governments participate: France, Netherlands, UK, Germany and Sweden.

8 Sourced under circumstances similar to those in footnote 4.

operators disclose their ability to implement already standardized privacy and security features. BEREC could work with such capacity monitoring in a manner similar to the already wide-spread performance measurements for network coverage and broadband speed. This could also fit with the proposed *Focus: End-User Perspective* Priority 7. ARTICLE 19 would be open to work with BEREC to identify such features, in order to strengthen the capacity of the EU mobile networking sector in the fields of security and human rights.

As we have raised in previous consultations, we believe that BEREC – similar to other public authorities – must seek continuous participation in, and interaction with, technical standards setting bodies to ensure a high level of protection for European consumers, businesses and verticals. Any restriction of fundamental rights, such as a limitation of a European citizen's or business' security, privacy or freedom of economic activity, must be proportional and necessary. BEREC should consider participating in technical standardization bodies in order to ensure that objective, hard security features, such as end-to-end encryption, protection against fake base stations, data identifier minimization, and similar features, are built into the networks as such. Given the cybersecurity threats that face individuals and companies. BEREC should consider cooperating with ENISA in this regard.

We discourage BEREC from pursuing the perspective that end-consumer oriented security may only be impacted by the increased use of cloud services, as was proposed in the document underlying the Call for Inputs.

3. Competition at retail level:

If BEREC undertakes further work in this area, it could usefully coordinate its research efforts with those proposed under *Focus: Verticals Perspective* Priorities 2-4 and 9-10 as well as *Roll-out* Priority 1.

EU member state markets for mobile communications are so consolidated, with three or four operators per market, that similar issues of retail level competition will be facing both consumers and the vast majority of companies. Only a few, large industrial actors are able to benefit from regional licenses, fully-owned local networks and service autonomy. Therefore, while we welcome the entry of more local MNOs into the market, we caution BEREC to relax its attention to real competition as perceived by consumers.

BEREC should explore whether wholesale level service guarantees are necessary to

ensure that downstream retailers can provide services as lawfully mandated to EU consumers and businesses. A network slice operator would for instance, by virtue of operating only on a slice, be entirely at the mercy of the quality of service techniques and other service characteristics determined by the network operator.

We wish to reiterate our position shared by ARTICLE 19 with BEREC in its January consultation on a draft BEREC Common Position on Mobile Infrastructure Sharing:

"Infrastructure-based competition is a form of service-based competition in the mobile sector and we believe BEREC's goals of benefiting European consumers would be served from a deeper reflection by BEREC on this point. /.../

Roll-outs of new technologies are made homogeneously over a market for mobile technologies. The 3G and 4G/LTE roll-outs were performed by different MNOs concurrently, and MNOs were not, in fact, competing with each other on the merits of their respective technologies, but only on the merits of the services they were able to provide through their new networks. Because all the providers have used the same technology, latency and speed have been the same.

Infrastructure-based competition in the mobile sector is therefore inherently different from infrastructure-based competition the way it has been understood for fixed networks."

Taking steps towards ensuring that a larger range of network operators can be simultaneously active on different member state markets, is one way of moving mobile networks into the relatively more competition-friendly architecture of current fixed networks. We also maintain our support for stronger national roaming obligations:

"ARTICLE 19 recalls current examples of national roaming, as investigated by ENISA in 2013.[9] It is instructive that markets with stronger national roaming obligations, that are neither time-limited nor restricted to 2G networks, appear to be capable of serving their consumers with more diversity and higher quality of services."

4. Competition at services level:

The Open Internet Regulation of the European Union[10], presumptively, guarantees

9 ENISA, National Roaming for Resilience, National roaming for mitigating mobile network outages, November 2013.

10 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'

that EU consumers of broadband services are able to access services of their choice.

We recall, in this regard, the importance of access to internet connectivity in order for individuals to exercise their human right to freedom of speech, freedom of opinion, and freedom of assembly, as emphasized by successive UN Special Rapporteurs charged with investigating this matter, as well as by the UN Human Rights Council in its declarations[11].

Against this background, it continues to be imperative that 5G technologies do not cause end-users to suffer a lack of diversity and choice. In particular, regulators should ensure that network slicing is not used as a pre-text for limiting the availability of internet services to end-users.

In fact, the technical capability of 5G to provide multiple isolated virtual networks ("network slices") to end-users over the same infrastructure which may have differing QoS characteristics opens up new business models to operators when providing IAS to end-users. In particular, operators may provide multiple slices of the "Enhanced Mobile Broadband" (eMBB) type with such differing QoS characteristics. In analogy to BEREC's opinion on the lawfulness of providing multiple subscriptions with differing QoS characteristics[12], the question of whether such a product would have to be assessed as making use of traffic management under Article 3(3) of Regulation 2015/2120, or as separate IAS, each subject to Articles 3(1) and 3(2) of the Regulation, depends on the application-agnostic accessibility of the different slices.

This dimension of application agnosticism moves into focus the transparency and configurability of the use of network slices by end-users on their terminal equipment. Only where end-user equipment allows end-users to configure the use of network slices in a transparent manner, and make autonomous decisions as to which traffic should make use of which slice, the access to these slices should be considered application-agnostic.

---

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.*

11 See, among others: Joint Declaration on Freedom of Expression and the Internet, UN Special Rapporteur on Freedom of Opinion and Expression (Special Rapporteur on FOE), the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 1 June 2011; Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, A/HRC/32/L.20, adopted on 27 June 2016. For a comprehensive analysis of the topic see also: ARTICLE 19, Getting connected: Freedom of expression, telcos and ISPs, Policy brief 2017, available at: https://www.article19.org/wp-content/uploads/2017/06/Final-Getting-Connected-2.pdf.

12 BoR (18) 244, pp. 7-8.

Thus, because 5G network slices can be used either to provide multiple IAS or institute traffic management on a single IAS, we suggest that BEREC should inquire end-user equipment manufacturers, operating system and firmware vendors, and operators as to the implementation and configuration of network slices on terminal equipment and publish a report about its findings.

5. State aid/coverage obligations:

BEREC should closely work with DG COMP to ensure state aid rules are not violated and to enhance legal certainty for actors. BEREC could contribute with further study, to informed policy to be adopted by DG COMP, possibly in the form of guidelines.