CDT Recommendations for BEREC Guidelines

1. Exemptions from content monitoring restrictions require more stringent safeguards

1. **Section 81** provides an exemption, for security purposes, to the restrictions on content monitoring set out in **section 66**.
2. We are concerned that this exemption, which might allow internet service providers (ISPs) to continuously monitor traffic and look beyond the header data to do so, provides an opportunity for abuse of the regulation by ISPs. We are also concerned that the caution against using the security exception to circumvent the regulation set out in **section 83** is too weak.
3. We recognise that such monitoring can be essential for ensuring the security of a network. For that reason we do not recommend that BEREC narrow **section 81** any further.
4. Recommendations:
    a. Information gathered under this exemption be subject to stringent data destruction/security protocols that ensure it cannot be used for any other purpose.
    b. BEREC should make clear to National Regulatory Authorities (NRAs) that the same stringent restrictions should apply to a contractual partner providing security services to an ISP.

2. Content interference and alteration restrictions on ISPs should be more detailed.

1. **Section 74 and 75** prohibit the alteration of content (including advertising) by ISPs as part of their traffic management practices.
2. We welcome the restrictions set out in **section 74 and 75** which prevent interference with content and services by ISPs while emphasising the right of end users to make use of ad-blocking software is not affected by this regulation.
3. Users do not and should not expect content or services to be interfered with by an ISP without their explicit consent.
4. Recommendations:
    a. Make it clearer to NRAs that interference by ISPs with content is prohibited under the regulation absent explicit user consent.
    b. Make it clearer in the non exhaustive list set out **section 75** that the restrictions on ‘**alteration’** and **‘interference’** of content by ISPs

encompass the *insertion (otherwise known as injection)* of content by the ISP (such as the ISP's own adverts).

   c. Clarify that the seven principles are ONLY allowed under the three exceptions to the traffic management rules, but are not allowed for any purpose other than exceptional traffic management.

3. Tethering should not restrict a user’s choice of terminal equipment.

1. CDT agrees with **section 25** of the guidelines where it states that *‘the practice of restricting tethering is likely to constitute a restriction on choice of terminal equipment’*
2. We welcome the clarification that an ISP which prevents, punishes or charges a user extra to access their phone’s internet connection with different terminal equipment, such as a laptop, will be in violation of the regulation.
3. We believe that preventing such technically unnecessary, commercially driven, tethering restrictions will have profound and positive effect on user choice in the European Union.
4. Recommendations:
   a. BEREC should ask NRAs to examine operator tethering policies in their markets.
   b. BEREC should highlight that blunt ways of management related to user choice of terminal equipment, like caps, are less desirable than more sophisticated means such as traffic shaping.
   c. BEREC should collect and compare ISPs justifications for *‘objective technological necessity’* to ensure the consistent application of the regulation.

4. Guidelines for NRA assessment of commercial practices should be more detailed.

1. We believe that the document does not currently provide sufficient clarity for NRA’s to properly, and consistently, determine what or does not constitute a ‘material’ reduction in user choice.

2. **Sections 42-45,** which discuss analytical factors that largely align with CDT's own analysis,[1] provide some limited guidance to NRA's on assessing commercial practices such as zero rating. However, **Section 42** states that *'It is not the case that every factor affecting end-users' choices should be considered to limit the exercise of end- users' rights under Article 3(1)*" and that *"Such restrictions would need to result in choice being materially reduced,"* but does not give any guidance as to what constitutes a "material" reduction.
3. Recommendations:
    a. BEREC should clarify what does and does not constitute a "material" reduction in user choice.
    b. BEREC should provide more guidance on how NRAs should determine what does and does not constitute;
        i. a Content and Application Provider (CAP) being materially discouraged from entering the market
        ii. 'other material harms to competition in the market'

5. Close examination of ISPs promotions is required to ensure that bundled offerings do not evade zero rating rules.

1. **Section 33** states that an ISP may bundle the provision of an internet access service (IAS) with an application and that such bundling should not be considered zero rating **unless *traffic* for the bundled application is priced differently or subject to preferential traffic management.**
2. We agree that such bundling - where the price ordinarily paid to the provider of an application is bundled into the price of the IAS - does not constitute zero rating provided the two above conditions are met. We believe that bundling of applications is a valid way of attracting new users and that ISPs should be free to offer promotions that give them an edge in the marketplace.
3. However, there is a risk to the regulation, because, in such circumstances there will be a strong commercial incentive for the ISP to ensure the user experience of their promoted application - and therefore pressure to give it preferential access to network resources;
4. Recommendations:
    a. For clarity, **section 33** should state that that the regulation permits offering free (or subsidised) access to an application *for a user* but does not does not permit offering free (or differently priced) data *for the application.* I.e a bundled offer may

[1] Erik Stallman & R. Stanley Adams IV, *Zero Rating: A Framework For Assessing Harms and Benefits*, Center for Democracy & Technology (Jan. 2016) available at https://cdt.org/insight/zero-rating-a-framework-for-assessing-benefits-and-harms/.

subsidize an application's subscription price, but not the data usage associated with that application.

b. NRAs need to take great care to ensure that when an application is being bundled with the IAS price that it is free (or subsidised) access to an application to a user, and *not* also free traffic for the application that is in fact being offered.

6. Additional safeguards would help protect improvements in the quality and capacity of Internet Access Services against encroachment by specialised services.

1. **Sections 117-121** generally protect the quality of IAS against detrimental effects from the development of specialised services.
2. Though setting the existing average IAS quality as a minimum standard might guard against specialised services causing *decreases* in IAS quality, it will not incentivise ISPs to invest in improving network capacity or transmission quality for IAS. Rather, it creates an incentive for ISPs to develop specialised services as replacements for applications and services currently provided via IAS and build capacity for those specialised services.
3. It is CDT's position that, while specialised services may provide benefits in certain applications, ISPs should be encouraged to continue to improve network capacity and performance for internet access services. IAS capacity and quality should continue to grow alongside network improvements for specialised services.
4. Recommendations:
    a. In determining whether specialised services are "not to the detriment of the availability or general quality of IAS," NRAs should consider whether specialised services are undermining investment and innovation in IAS or otherwise negatively impacting the improvement of IAS.

7. Encryption and net neutrality

1. CDT welcomes the clarification set out in **Section 61** that *'Encrypted traffic should not be treated less favourably by reason of its encryption.'*
2. We strongly support the principle that encrypted traffic should not be subject to discriminatory traffic management simply because that traffic is encrypted.
3. Greater uptake of secure protocols by service providers requires that service provided by such protocols are of comparable quality to their insecure equivalents.