Your response

Zero-rating

Question	Your response
Question 1: Do you agree with our assessment of zero-rating offers and our proposed approach?	The Internet Society supports the Court of Justice of the European Union (CJEU) interpretation of zero-ratings and BEREC's subsequent revised guidelines on zero-rating offers. We encourage the UK to continue to align its guidelines with these outcomes under the Open Internet Regulations. The CJEU ruled that zero-rating offers violate net neutrality and are illegal under EU law. The ruling clarified that the general obligation to treat all traffic equally under net neutrality is not limited to technical traffic management practices but also applies to commercial practices of Internet Service Providers (ISPs), including the practice of zero-rating. We agree with this conclusion. BEREC's revised guidelines clarified that zero-rating offers for specific applications or categories of traffic negatively impact the open Internet. We agree with this conclusion and emphasize the potential negative impact of zero ratings, including potential market consolidation by dominant players and the departure from the general-purpose nature of the Internet that has fueled decades of innovation and growth.
Question 2: Do you agree with the criteria we use to define Type One, Type Two and Type Three zero-rating offers and our proposed approach to such offers?	We discourage the criteria and approach used to define the zero-rating offer tiers. Creating categories of content for zero-rating offers not only impacts net neutrality but also creates practical challenges that could harm the Internet and distort competition. For example, "video streaming services" fall under the "Type Two" zero-rating offer and would face practical implementation challenges. This is because numerous companies offer a combination of music streaming, gaming, E-sports, and social media services in combination to video streaming.

	Classifying which content would qualify for the zero-rating offer is challenging, classifying which traffic corresponds to the qualifying content would be even more difficult. These issues could distort competition with companies that offer services across categories more likely to qualify for a zero-rating offer, giving them a competitive edge. This issue would be compounded by the requirement that providers must first apply (and meet certain administrative, technical and potentially financial requirements) to be considered for zero-rating offers. Large companies are best positioned to benefit from this "burden of awareness" given their larger resources whereas smaller providers, especially those operating from elsewhere in the world, would face new barriers.
Question 3: Do you agree with the approach in our guidance in Annex 5 in relation to zero-rating?	N/A
Question 4: What are your views on whether zero-rated content should be able to be accessed once a customer's data allowance has been used up?	N/A
Please provide any further evidence you have to support your responses.	
The Internet Society supports the Review's rejection of "sender-party pays" proposals that would enable Internet Service Providers to charge content providers for carrying or prioritising general Internet access traffic. The UK's rejection of these proposals will avoid unwanted consequences, including harm to the global and open Internet. The Internet's key strength lies in its ability to empower users to access all corners of the shared network of networks. The need for content providers to negotiate access to the user's ISP would damage this feature by limiting users only to the parts of the Internet that their contract allows for, potentially cutting users off from large sections of the global Internet. South Korea has implemented a sending-party pays regime which have resulted in inefficient traffic flows, high costs, low quality service, and delays in the employment of new infrastructure. Our analysis of the South Korean rules provides cautionary evidence that should inform decisions elsewhere in the world.	

Traffic management

Question	Your response

Question 5: Do you agree with our assessment of retail offers with different quality levels and our proposed approach?	N/A
Question 6: Do you agree with the approach in our guidance in Annex 5 in relation to differentiated retail offers, including transparency requirements, improved regulatory monitoring and reporting of retail offers with different quality levels as well as the general quality of the internet access services?	N/A
Question 7: What are your views on a more permissive approach towards retail offers where different quality levels are content and service specific?	We disagree with this approach. Retail offers that differentiate on quality levels are acceptable when they are application and content agnostic. Retail offers that differentiate quality levels based on the category of services or content negatively impact the open Internet and is in direct violation of net neutrality. This approach could cement the dominance of existing digital players and could create barriers to future UK innovation as the even playing field created by the general-purpose nature of the Internet is lost.
Question 8: Do you agree with our assessment of how traffic management can be used to address congestion and our proposed approach?	N/A
Question 9: Do you agree with the approach in our guidance in Annex 5 in relation to the use of traffic management to address congestion, including transparency requirements, improved regulatory monitoring and reporting of general network performance metrics, the use of traffic management and the impact on service quality?	N/A
Question 10: What are your views on a more focused approach to traffic management to address congestion?	N/A
Please provide any further evidence you have to support your responses.	

Specialised services

Question	Your response
Question 11: Do you agree with our assessment of specialised services and our proposed approach?	N/A
Question 12: Do you agree with the approach in our guidance in Annex 5 in relation to specialised services, including transparency requirements, improved regulatory monitoring and reporting of the need for optimisation of a service, the general performance of internet access services and the impact of specialised services on the quality internet access?	N/A
Please provide any further evidence you have to support your responses.	

Scope of the net neutrality rules, terminal equipment and public interest exceptions

Question	Your response
Question 13: Do you agree with our assessment of the terminal equipment rules and our proposed approach?	N/A
Question 14: Do you agree with our assessment of internet access services provided on aeroplanes, trains, buses and coaches and our proposed approach?	N/A
Question 15: Do you agree with our proposed approach to emergency 999 communications services and that we should consider amending the GCs to achieve this?	N/A
Question 16: Do you agree that ISPs should be allowed to block scams and fraudulent content and provide in-network parental controls and content filters?	The Internet Society believes that any such powers must be clearly scoped to rule out actions from ISPs that could threaten user privacy and autonomy.

	It is important that regulation clearly distinguish between blocking and filtering that happens “in-network” versus “over-the-top”. Doing so ensures that countermeasures are carried out by the most appropriate party for a particular goal. This increases accountability and trust in online intermediaries by clarifying who is responsible to whom, and for what. ISPs are well-suited for countering attacks on the network itself (as defined in the consultation document) such as denial of service attacks, botnet attacks, and IP address spoofing. ISPs can use “in-network” tools to monitor network traffic and identify these attacks without violating net neutrality and without access to the contents of communications. ISPs, however, are not best suited for countering the other two forms of attack defined in the consultation document, namely attacks on services delivered over the network, or attacks on users’ devices such as e-mail abuse, spam, phishing, and malware. Although these attacks are network borne, they do not operate at the network level. Since they exploit “over the top” services, the ISP should not, by default, be the regulatory enforcement point. Instead, these attacks are best countered using “over the top” tools, which tend to require access to the contents of network traffic. Network traffic patterns (i.e. communications metadata, not communications contents) are a legitimate indicator of attacks, and can be monitored by ISPs without violating the principle of net neutrality. Parental controls that operate on metadata (for instance, using blocklists of known malicious sites) would usually fall into this category. An exception to this generalization is needed to distinguish between user-operated and ISP-operated “in-network” controls. The Oxygen 2022 research report cited in this section found that most respondents favoured controls that they could operate at their own discretion, meaning that while ISPs may supply these tools, they should not

	control them directly. Users must be given the explicit opportunity to opt-in to such controls, so that principles of transparency and consent are respected. ISPs legitimately require access to network traffic metadata. However, we believe that when users apply “over the top” tools at their own discretion, that ISPs should not have access to the data used to operate those tools. Likewise, ISPs should not have the means to render encryption or other confidentiality tools ineffective. Limiting ISPs to clearly defined “in-network” tools would better ensure user privacy and autonomy and contribute to increased Internet security and trust.
Please provide any further evidence you have to support your responses.	