

In Response to the
Body of European Regulators of Electronic Communications Consultation on
Common Approaches to the Identification of Network Termination Point in Different Network
Topologies

Comments of the Center for Democracy & Technology and Public Knowledge
21 November, 2019

The Center for Democracy & Technology (CDT) and Public Knowledge (PK) thank BEREC for the opportunity to provide input on this issue.

CDT is a nonprofit public interest group that seeks to promote free expression, privacy, individual liberty, and technological innovation on the open, decentralized internet. CDT supports laws, corporate policies, and technical tools that protect the civil liberties of internet users. CDT represents the public's interest in an open internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

Public Knowledge is a nonprofit technology policy organization that promotes freedom of expression, an open Internet, and access to affordable communications tools and creative works.

Defining the network termination point (NTP) matters. It impacts the scope of regulation for ISPs, the choice and availability of terminal equipment for end users, network security and management, and data privacy. As we consider how best to serve internet users' needs, it is therefore appropriate and necessary to achieve a common approach to NTPs and to provide common guidance to the national regulatory authorities responsible for implementing regulations. CDT and PK appreciate BEREC's thoughtful and thorough approach to this issue and offer the following responses to the points raised in the consultation document.

In general, CDT and PK approve the proposed guidelines to help national regulatory authorities (NRAs) approach defining the NTP from a common perspective. However, to achieve a more harmonised approach and market, CDT suggests that BEREC consider designating either Point A, B, or C as the default definition of the NTP. Overall, **CDT and PK support point A as the best choice for the NTP**. We recognize that the structure of BEREC's proposed guidelines allows national regulatory authorities to determine the NTP definition on a more flexible basis. However, CDT and PK suggest that BEREC consider proposing Point A as the default NTP, with the option for NRAs to make a different determination, for example where certain network topologies require a different assessment.

Further, we suggest that BEREC consider a slightly different description of Point A. Rather than describing Point A as depicted in Figure 2, essentially "before the modem," we propose that Point A should be considered the first point at which the customer can attach standardised

network interface equipment, such as devices that support DOCSIS or Ethernet. This aligns the NTP more closely with both the physical space within end users' control and with end users' understanding of network topologies. We understand that this may, in some cases, merge Points A and B and in others merge Points B and C, but it would also reduce confusing abstractions like defining the NTP as a point residing inside a single piece of terminal equipment on the customer premises.

Our perspective as civil society organisations allows us to consider the users' goals and needs as our fundamental touchpoint, and that perspective may be different from internet service providers who are obligated to pursue shareholder goals. Given the standardized nature of internet communication protocols, in most cases we are dubious that ISPs are likely to demonstrate sufficient objective technical necessity to justify their own determination and control of TTE equipment used by their subscribers. Additionally, the pro-competitive aims of Directive 2008/63/EC weigh strongly against any NTP other than Point A.¹

However, because even a default definition of NTP at Point A would not preclude ISPs from providing, offering, or suggesting particular terminal equipment to their subscribers, BEREC should also ensure that ISPs supply equipment that is capable of supporting their highest advertised data speeds and offers up-to-date security protections. ISPs should not suggest or supply equipment that limits user's maximum speeds or other performance aspects, for example, as a method of controlling subscribers' network usage. Additionally, ISPs should only supply or suggest equipment that is capable of supporting new firmware updates, such as are necessary to improve either security or performance. When ISPs supply or suggest particular terminal equipment, they should provide to the NRAs and to end users the relevant technical specifications of the equipment, including maximum data speeds and other metrics related to the users' interests in internet access and network security.²

The remainder of CDT's and PK's responses to BEREC's proposed guidelines are as follows:

3.1.3 Regulation (EU) 2015/2120 - CDT and PK support Point A as the best option because it gives users the greatest number of choices and greatest control over the TTE in their own homes. Although other NTP placements could potentially satisfy the regulatory language in Article 3(1) in conjunction with the definition of "terminal equipment" in Directive 2008/63/EC (Art. 1(1)), Point A is best aligned with the spirit of the Open Internet regulation because it maximises users' control and choice while also reducing opportunities for ISPs to exert unnecessary control over users' internet access and local networks.

¹ Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in TTE, OJ L 162/20 of 21 June 2008.

² This obligation would also align with Directive 2008/63/EC, Recital 8, but here the consumer-facing disclosures should be explicitly required to ensure better understanding of equipment limitations and facilitate comparisons between competing options.

3.2 Impact on TTE Market - As BEREC notes in the consultation document, identifying Point A as the NTP likely will result in more end users choosing and purchasing their own modems and routers.³ The diversity of end user needs and preferences will encourage producers of modems, routers, and other network equipment to develop a wider array of options for the retail market, resulting in greater choice for consumers. This should create a more competitive market for home networking equipment and also drive manufacturers to develop faster, more reliable, more secure equipment at lower costs to consumers. Additionally, a more diverse technical ecosystem provides a more complex attack surface and limits the impact of cyberattacks on network equipment.⁴ CDT and PK agree with BEREC's assessment of the market impacts of choosing Point A as the NTP and support Point A as the best way to enable more choices for internet users while also fostering innovation and competition in the TTE market.

3.3.1 Interoperability between public network and TTE- The considerations BEREC proposes to ensure interoperability of TTE and NTP characteristics are valid. However, CDT and PK are unconvinced that regulatory oversight will be necessary to ensure interoperability of TTE with internet access services and continue to support Point A as the optimal default location for NTPs in all member states.

The internet's basic structure is one that enables networks to send and receive information. As such, today's internet depends on standardization to allow joined networks to send and receive information and to ensure that information streams are delivered efficiently to the appropriate endpoints. For this reason, the format, routing, and delivery methods required to send information between any given endpoints on the internet are already harmonised. Therefore, the basic functions of terminal equipment are the same, regardless of which access network they are attached.

This common functionality combined with an interest in developing popular products creates a strong incentive for TTE makers to design their consumer-facing products so that they meet the technical requirements of access network operators. Additionally, the obligation in Directive 2008/63/EC, Art. 5 for member states to "ensure that all specifications for terminal equipment are formalised and published," means that all TTE producers should have sufficient technical information to design and build compatible products for any given access provider's network. From this perspective, CDT and PK believe that market forces and standardized protocols are sufficient to ensure that TTE makers will produce safe and interoperable products, regardless of which NTP location is selected.

In theory, both ISPs and TTE manufacturers share strong interests in interoperability, regardless of NTP location. However, to the extent that ISPs wish to participate in the market for TTE, they may have an incentive to design their networks to require proprietary equipment for which they are the sole producer. ISPs should be discouraged from configuring their networks so that their

³ BEREC Guidelines on Common Approaches to the Identification of the Network Termination Point in Different Network Topologies, BoR 19 (181) ("BEREC NTP Guidelines"), at 3.2.1, para. 35.

⁴ See, *infra* 3.3.3.

NTPs require specific, proprietary equipment for purposes of market control. BEREC's guidance that "objective technical necessity" must be shown to justify "obligatory equipment" should prevent this undesirable outcome, however any such purported technical necessity should also be evaluated in light of its relationship to the overall functionality of the TTE and the internet access service. For example, an alleged technical necessity that is only necessary to support an ISP's data collection from a piece of TTE, but does not impact the user's ability to access the internet should not satisfy the condition.

For some fiber optic network connections, it may be the case that third-party equipment like optical modems (or optical network terminals) are not available in consumer retail markets. In other cases, such as fiber-to-the-node or fiber-to-the-building, these optical-to-digital modems are not accessible to end users at all. In these cases, we propose that Point A should be considered the point at which the customer can attach standardised equipment, such as devices that support DOCSIS or Ethernet. Additionally, to the extent that some other mode-shifting equipment is necessary to allow users to connect standardised equipment, ISPs should be prohibited from charging customers for that equipment.

3.3.2 Simplicity of the operation of the public network - As noted above, TTE makers have a strong incentive to produce equipment that is interoperable with all networks. Likewise, they should be encouraged to coordinate with ISPs in advance of any network-wide change in management or operational practices and to develop software updates as necessary to preserve compatibility of existing equipment with new network protocols. More simply, users should not need to buy new TTE to adapt to a protocol change, but they should be made aware of any available updates to ensure forward compatibility.

With the NTP defined at Point A, timely maintenance of terminal equipment admittedly requires higher levels of coordination among equipment makers, ISPs, and subscribers than if the ISP controls the firmware of users' modems, but preserving user choice of home TTE aligns more closely with open internet principles and Article 3(1) of Regulation (EU) 2015/2120. Therefore, despite some increase in the complexity of network operation and equipment maintenance, CDT and PK continue to suggest that BEREC's guidelines recommend Point A as the default NTP option.

3.3.3 Network Security - Network security is, of course, of paramount importance. We recognize BEREC's perspective that giving the ISP control over more of the TTE could make a unified security effort more efficient. However, this also depends on the ISP taking timely and appropriate steps to ensure security, and that does not always happen. As BEREC notes, the consequences for an insecure piece of TTE are greatly magnified in the situation where all NTPs have common TTE; a bit like putting all of one's eggs in the same basket. By contrast, greater diversity of TTE diminishes the overall impact of some insecure equipment on a network.⁵

⁵ BEREC NTP Guidelines at para. 90.

If, instead, the NTP is defined differently, at Point B or Point C, consumers are left without recourse when ISP controlled TTE is compromised, but their own equipment, including CPE and connected devices beyond the NTP, is likely to be impacted by the compromise. The choice here balances user choice and control of the devices in their homes against the efficiency of allowing the ISP to dictate security updates for modems and routers. CDT and PK suggest that the benefits of users' choice and control over the TTE in their homes, especially from a security perspective, outweigh the risks associated with vulnerable equipment at network endpoints and that Point A remains the best option for a default specification of the NTP.

In any case, either TTE makers or ISPs should take reasonable steps to notify end-users of necessary security updates. Where users are responsible for security updates, ISPs could offer some information as well as incentives to encourage users to take steps to secure their equipment.

3.3.4 Data Protection - In terms of data protection, the implications of positioning the NTP at Point C are significant because including local network traffic as part of the public internet raises several concerns. Even if ISPs are prohibited from listening to or otherwise intercepting communications,⁶ and even if end-users take steps to encrypt their local traffic,⁷ it may be impossible to encrypt all local traffic. For example, end-users may have little or no control over the way some connected devices transmit information, whether outbound to the public internet or sent to another device on the local network. Likewise, there are strong policy reasons to keep the public internet and users' local networks both logically and legally separate. For example, even though the legal prohibitions mentioned in the proposed guidelines should stop ISPs from monitoring local network traffic, it may be difficult for end-users to detect such activity. Likewise, there may be practical issues with ISPs and users sharing control over networking equipment and the configuration thereof. Ultimately, preserving end-users' sole control over local data traffic weighs strongly in favor of Point A and we urge BEREC to recommend this as the default NTP.

3.3.5 Local Traffic - The legal and practical considerations recognised by BEREC in the proposed guidelines also weigh strongly in favor of defining the NTP at Point A, in terms of both the privacy concerns above and the practical issues with separating local and outbound traffic.

3.3.6 Fixed Wireless - Even for fixed wireless internet access services in which there is no wire termination point at the customer's premises, CDT and PK support Point A as the best location for the NTP. In the same way that mobile device manufacturers can design phones to accommodate multiple carriers' networks, so too can TTE makers produce home equipment capable of interoperability with multiple fixed wireless network providers. Likewise, ISPs should

⁶ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L201/37 of 12 July 2002.

⁷ As suggested in the BEREC NTP Guidelines at para. 110.

be discouraged from requiring specific, proprietary TTE for fixed wireless service unless there are compelling technical reasons to do so. To do otherwise affects competition unduly. But the current mobile broadband and voice market, both for carriers and device makers, indicates that interoperable equipment is possible and produces more choice for consumers. Although this issue also implicates some technical aspects of device and network authentication protocols and practices, those issues are better addressed through standards setting bodies and appear to be beyond the scope of this consultation.

Respectfully submitted,

Stan Adams
Open Internet Counsel
Center for Democracy & Technology
sadams@cdt.org

John Bergmeyer
Legal Director
Public Knowledge
john@publicknowledge.org