INTUG

Public Consultation on the Open Internet and Net Neutrality in Europe

Response from The International Telecommunications Users Group (INTUG)

Executive Summary

INTUG welcomes the opportunity to provide a response to the European Commission's public consultation on the Open Internet and Network Neutrality in Europe, on behalf of business users of communications. Future economic growth and social inclusion within the EU will depend significantly on access to the Internet and ubiquitous use of content, applications and services. It will also depend on openly available and competitively supplied fibre-based Next Generation Access (NGA) networks and related services. INTUG has provided a separate response to the consultation on that issue.

"Open Internet and Net Neutrality" must be clearly defined and consistently interpreted to ensure an effective outcome from the consultation. It is part of a fundamental principle of open communications which has broader scope than the issues raised in this consultation. Absolute neutrality in ICT terms means that any choice of communications service or information technology component does not, per se, reduce other choices available to the user for different services or components. The scope of this definition would include all devices, connecting services, management tools, content, applications and other elements of the ICT landscape. This is, of course, rarely fully achievable, given the step change nature of some progress, and the need for affordable migration. Disconnection from the past is inevitable in many cases, for example with the move from analogue to digital TV. However, the principle should still be maintained, and attempts made to mitigate, if not eliminate, the impact on existing investments.

This principle of neutrality should be applied to the current consultation, as the logic applies equally to simultaneous supply of ICT elements by different providers. The choice of one provider or one ICT element should not restrict the choices available elsewhere in the ICT landscape. Connecting directly or indirectly to any item of ICT, from any provider, should not in an ideal world impact on past, current, or future choices for similar elements in a different place, or for a different purpose, or on other elements that must interwork with it. The key objective here is seamless, timeless interoperability.
This extends to, but is not limited to: functionality, operability, total quality, information content, display capability, or any other characteristic of the connected technology. Indirect connection refers to a piece of technology which is connected further away, via one or more intermediate devices, and which must also not have its capabilities affected by the choice of a piece of technology anywhere in the connection chain.

Having established the fundamental functional issues which underpin assessment of user

requirements, which apply to public and private sector enterprises, to SMEs and to mass market end consumers, it is possible to move on to the specific application of this principle to the issues concerning an Open Internet and Net Neutrality.

The overriding issues for users are:

- differentiation, discrimination and transparency.
More specifically, the key questions, which must be addressed, are as follows:

- in what circumstances is it acceptable, and possibly desirable, for an element within the ICT landscape to be provided on a differentiated basis to different customers, and/or at different times, and/or in different places, and/or based on different contractual terms?

- in what circumstances is it acceptable, if ever, for a service provider to discriminate in the provision of a communications service or technology component, in terms of availability, functionality, performance, quality and/or manageability, between business partners and/or customers, and/or other service providers?

- how transparent will the differentiation as defined above, and discrimination (if allowed) be, in advance, at the time, and after the event, in terms of specific information provided to business partners, customers, competitors, regulators, investors and/or government?

In addressing these key questions, it is important to recognise that full recognition is given to the different and distinct needs of private and public enterprise customers, compared to those of the mass market consumer. The assessment of whether or not a problem exists must not be confined to analysis of individual site connections in single Member States.

The multi-site, multinational connectivity requirements of enterprises demand a greater level of Open Internet and Net Neutrality. End-to-end connectivity must not be subject to denial of application use, or blockage of content, due to the actions of one service provider within the connectivity chain. Mission critical business process cannot tolerate the impact of such differentiation or discrimination in the same way that an individual consumer can, since the latter can use a competitive retail market to change supplier, whereas an enterprise customer cannot, in such circumstances.

The term “traffic management” is used to justify actions taken by service providers who deal with traffic selectively, to achieve desired performance outcomes, particularly during periods of congestion where bandwidth is inadequate, or where unacceptable latency would result. Consumers experience traffic management in everyday life, for example on high speed roads, where variable speed limits are applied, lanes are closed or reserved for public transport (or dignitaries during the Olympics), and traffic calming measures are implemented through speed bumps and chicanes. Fuses disconnect equipment to protect overload in electrical systems. These processes are transparent and visibly implemented.

However, restricted lanes for certain makes of car would not be tolerated. Circuit breakers triggered by the brand name of an electrical appliance would be unacceptable. But this kind of non-neutrality exists on the Internet today. And the blocking of certain applications and content cannot be justified, unless it is demonstrable that they can be clearly classified

by type of application or content, and not by the supplier or service provider. The key is to have an agreed definition and classification system for applications and content, which is consistently applied. This would not group together all peer-to-peer applications and block them all, when only some threaten critical latency or service integrity. Only then can traffic management be used acceptably, without becoming anti-competitive discrimination.

Discriminatory non-neutrality must not be allowed by disguising it as operational traffic management in situations of transient technical overload, emergency or security breach.

One final point must be stressed in terms of the risk of inappropriate traffic management, and that concerns remedies in the event of breach of intellectual property rights. These can in some situations become in conflict with user rights of access. This controversial issue threatened to obstruct final agreement on the Framework review, requiring difficult compromises between the Council of Ministers, the Commission and Regulators.

This issue also highlighted a significant difference between what might be an appropriate approach for a single site Internet user and an enterprise customer or Internet service provider. Summary disconnection as a remedy, for example following repeated illicit file sharing, would be wholly inappropriate, disproportionate, unworkable and unacceptable for enterprise customers and ISPs, who cannot control the behaviour of individual transient users connected to their networks. In this instance, net neutrality is non-negotiable.

In terms of the European Union, it is essential, if a Single Market in ICT is to be created effectively, that the approach to net neutrality should be the same in all Member States. Current levels of fragmentation and dysfunctionality guarantee that, for most enterprise customers, the present situation provides neither an Open Internet nor Net Neutrality.

International Telecommunications Users Group (INTUG)

The International Telecommunications Users Group (INTUG) represents the interests of business users of telecommunications. These include some of the world's largest financial institutions, car manufacturers, pharmaceutical companies, fast moving consumer goods enterprises, retail and distribution companies, and small and medium enterprises (SMEs).

The INTUG community includes user associations in many large Member States, including Belgium, Denmark, France, Germany, Spain, the Netherlands, Sweden and the UK, and the multinational user group EVUA. Each group represents public and private sector customers of communications service providers.

Confidentiality and Contact information

Nothing in this submission is confidential and the contents can be considered to be in the public domain. The submission is available on the INTUG web site at http://intug.org. This submission should be read in conjunction with INTUG's response to the consultation on the Next Generation Access (NGA) Recommendation. The contents of that submission have not been repeated here. An INTUG press statement accompanies this response.

Comments should be addressed to:

Nick White, Executive Vice President
International Telecommunications Users Group (INTUG)
nick.white@intug.org
Tel: +44 20 8647 4858 Mobile: +44 77 1009 7638

INTUG

Public Consultation on the Open Internet and Net Neutrality in Europe

Responses to Specific Questions from the International Telecommunications Users Group (INTUG)

Question 1: Is there currently a problem of net neutrality and the openness of the Internet in Europe? If so, illustrate with concrete examples. Where are the bottlenecks, if any? Is the problem such that it cannot be solved by the existing degree of competition in fixed and mobile access markets?

INTUG Response: Absolutely YES. There is a major problem, due to the fragmented and dysfunctional fixed and mobile national markets operating within the EU today. This results in a complete inability for large, medium and small enterprises to build seamless transnational networks, let alone obtain comparable competitive bids from pan-EU suppliers in either market.

Individual mass market consumers also experience restricted choice of devices and blocked functions such as VoIP, an absence of transnational MVNOs on mobile networks, restrictions on access to information services and media on fixed networks, and non-disclosed performance discrimination by operators.

There are bottlenecks from lack of open and non-discriminatory access to wholesale broadband services, inconsistent and incompatible allocation of spectrum, complex Member State specific approval and licensing processes, inadequate peak capacity in core and backhaul networks and inter-operator transit points, device and content exclusivity within network operator services, and constraints on access to network management information.

The problem is too great to be solved by the existing degree of competition, such as it is, in either fixed or mobile access markets. It requires consistent co-ordinated ex-ante regulation within the context of the revised Framework Directive, to ensure critical bottleneck resources are expanded and are not monopolised by incumbents.

Question 2: How might problems arise in future? Could these emerge in other parts of the Internet value chain? What would the causes be?

INTUG Response: There is a risk that transposition of the Better Regulation and Citizens' Rights Directives, and the NGA Recommendation, into national law could result in problems arising in the future, and existing problems being exacerbated.

INTUG is concerned that loopholes in the NGA Recommendation could lead to the

remonopolisation of fixed access and a continued absence of effective competition in international fixed networks services.

The conflicts between user rights on security and privacy and intellectual property rights (IPR), in the context of illicit file sharing, have already highlighted the risk that basic Internet access might be denied by implementation of a remedy on an Internet Service Provider. This would be completely unacceptable for a business user.

Due to differences between individual Member State constitutions, this has already generated intense debate and changes in some national law to adjust the balance of responsibilities between rights holders and ISPs (reference the HADOPI law and application of the Digital Economy Act in the UK). It is essential that a consistent position on these matters is reached in all Member States.

International business processes must share data across borders. EU privacy laws restrict the handling of personal information on customers, employees, suppliers and shareholders. Such information cannot be transferred to non-EU countries with inadequate levels of data protection. This limits outsourcing of applications which process personal data. There must be a clear legal framework for such issues.

Question 3: Is the regulatory framework capable of dealing with the issues identified, including in relation to monitoring/assessment and subsequent enforcement?

INTUG Response: The regulatory Framework established by the revised Directives and associated measures should provide capability for monitoring and assessment. However, history suggests that significant market power operators are very adept at delaying the impact of regulation, for example by appeals. Experience suggests that such actions have been sufficient to deter market entry by potential competitors and to damage the financial performance of those who do enter the market.

Enforcement after the event, whilst better than simply relying on ex-post regulation based on general competition law, is unlikely to be sufficient on its own to deal with the range of issues identified above.

The creation of BEREC offers the prospect of more effective enforcement and co-ordinated consistency between NRAs. Their work programme should include priority emphasis on tracking the progress, or lack of progress, in establishing and sustaining an Open Internet and Net Neutrality.

Regulation on its own is unlikely to be sufficient to guarantee equitable application of net neutrality principles, but useful measures, which might be applied, include:
- enforcement of transparency in contracted traffic management measures
- ensuring bottlenecks are not created by SMP providers to generate revenue
- elimination of discriminatory practices against competing suppliers
This needs to be accompanied by encouraging investment in adequate bandwidth.

Question 4: To what extent is traffic management necessary from an operators' point of view? How is it carried out in practice? What technologies are used to carry out such traffic management?

INTUG Response: As a general principle, "traffic management" is only essential where there is inadequate bandwidth to cope with overall demand or congestion, especially in the backhaul and local loop. Other instances of traffic management are largely driven by commercial motives. Operators can exploit this to defer investment, to avoid cannibalising high margin leased line revenues, to pressure governments to offer state subsidies, to persuade regulators to give exemptions, and to generate additional revenue through offered layered Quality of Service.

Consistent delivery of total quality services by a network operator requires end-to-end service and network management. Such management is only possible with end-to-end access to network status and traffic management information.

This is necessary to enable the operator to adapt configurations and routes to cater for changes in traffic patterns, the incidence of peak loads, and the consequences of failures and associated remedial action, such as re-routing, re-transmission and use of alternative mechanisms.

End-to-end service is often outsourced to a systems integrator or virtual network service provider, who in turn requires access to network management information and tools used by the underlying service providers. Technology standards exist to facilitate such management, but resistance, and in some cases refusal on the part of some operators to grant access to network management facilities and information, handicaps the end service provider's ability to deliver contracted service quality.

Large enterprise users tend to adopt their own technology standards if they manage their own network service providers and may be able to demand contracted access to network management information. Mandatory standards to be adopted, and an obligation to provide information, is a minimum requirement. The rules used for traffic management by an operator should be transparent and disclosed to users.

Question 5: To what extent will net neutrality concerns be allayed by the provision of transparent information to end users, which distinguishes between managed services and services offering access to the public internet on a 'best efforts' basis, on the other?

INTUG Response: Whilst Net Neutrality concerns might be allayed to some degree by the provision of transparent information to end-users, it does not address the underlying issue, and is likely to be motivated by a desire to avoid the economic consequences of measures designed to speed up the introduction of universal access to high speed broadband. Transparency is necessary, but not sufficient.

Nevertheless, it is vital that transparent traffic management information is given to wholesale customers, systems integrators, virtual network operators, and national regulatory authorities (NRAs), to ensure operational procedures can be monitored by them for evidence of non-discrimination, and for compliance with advertised performance and contracted quality commitments.

Implementing a distinction between services offered on a "best efforts" basis and others is, by definition, not network neutral, but is acceptable in the context of the additional user welfare created by differentiated service quality options. This does, however, require that the characteristics of each is transparently disclosed before, during, and after service delivery, and is reflected in contracts, especially for public and private enterprise customers.

Question 6: Should the principles governing traffic management be the same for fixed and mobile networks?

INTUG Response: Absolutely Yes! The principles governing traffic management, in terms of the circumstances in which prioritisation can be applied, should be based on the same logic, but they may inevitably have to differ in implementation due to the nature of the services offered, the impact of service failures, and the legal and commercial obligations inherent in service provision.

Transparency of traffic management information, as discussed above, must be guaranteed for both fixed (wired and wireless) networks, and for mobile networks.

Question 7: What other forms of prioritisation are taking place? Do content and application providers also try to prioritise their services? If so, how – and how does this prioritisation affect other players in the value chain?

INTUG Response: Lack of transparency in current network operations limits ability to comment specifically on the forms of prioritisation currently taking place.

There is already widespread prioritisation executed by operators, supposedly to manage quality of service, but this could well be done in a manner which optimises service provider revenue and quality perception. This justification cannot be used, however, for blocking applications completely, as is the case with VoIP/Skype on some mobile networks. This prevents businesses from introducing international business processes based on such applications, since the processes can only reach Member States where such applications are not blocked.

As a further example, BSkyB prioritise through bundling of channels, through different price structures for different quality reception (e.g. HDTV), and through restrictive practices in the PayTV wholesale market, where it has SMP.

Undisclosed prioritisation to favour one customer over another, one contract over another, and perhaps even to ensure preferential performance for the provider's own services over those carried for competitors, affects other players in the value chain profoundly, but evidence of this taking place is hard to obtain, and is largely based on suspicion and hypothesis. However, it has been alleged by some competing operators and customers that such practices do occur.

Question 8: In the case of managed services should the same quality of service conditions and parameters be available to all content/application/online service providers who are in the same situation? May exclusive agreements between network operators and content/application/online service providers create problems for achieving that objective?

INTUG Response: The same options for quality of service and parameters should be available to all content, application and on-line service providers, including those of the network operator itself. There is a real possibility that exclusive agreements between network operators and providers will, by their nature and definition, make achievement of the aims of equivalence of quality, functionality and manageability, hard if not impossible to achieve, leading to anti-competitive discrimination.

Question 9: If the objective referred to in Question 8 is retained, are additional measures needed to achieve it? If so, should such measures have a voluntary nature (such as, for example, an industry code of conduct) or a regulatory one?

INTUG Response: Preservation of the basic principle of non-discrimination may well require applying some form of regulatory remedy, for example functional separation, as monitoring and accounting separation has proved largely ineffective to date. Voluntary self-regulation has not always been very successful in the telecommunications sector, and reliance on ex-post competition remedies has been insufficient. Whilst codes of conduct are to be welcomed as a gesture of good intent, a regulatory mechanism will be needed.

Question 10: Are the commercial arrangements that currently govern the provision of access to the Internet adequate, in order to ensure that the Internet remains open and that infrastructure investment is maintained? If not, how should they change?

INTUG Response: No. Manipulation of relative performance delivered to individual customers is already widespread, especially when dealing with peak traffic loads.

There are also numerous examples of denial of access to equivalent services for wholesalers wishing to compete via use of bottleneck infrastructure, and blockage of access to content for political and censorship reasons, beyond the prevention of access and distribution of harmful or illegal content. Infrastructure investment will be encouraged where usage opportunities are maximised, not by leaving regulatory loopholes permitting exclusivity, for example through co-investment or reciprocity.

Regulation should require open access on an equivalent non-discriminatory basis to competing service providers, and should disallow blockage of access to content or applications for commercial reasons. Inefficient duplicate access infrastructure investment should be avoided, rather than being forced upon new market entrants.

Question 11: What instances could trigger intervention by national regulatory authorities in setting minimum quality of service requirements on an undertaking or undertakings providing public communications services?

INTUG Response: On-line e-services, bring much needed improvements in overall efficiency, effectiveness and productivity. This is particularly welcome in today's economic climate. The absence of adequate facilities to enable such e-services could trigger national regulatory authorities to set minimum quality standards.

This could include latency maxima to serve the needs of communications networks supporting smart grid operations, or command and control components in public utility networks, such as water and gas pipeline distribution facilities.

Question 12: How should quality of service requirements be determined, and how could they be monitored?

INTUG Response: Quality of service requirements are best defined by customers, including public and private enterprises of all sizes, as well as mass market end-consumers. This will enable meaningful definition of quality measures, rather than technology indicators that have no relevance to the actual service being delivered. Headline downstream and upstream bandwidth measures are wholly ineffective.

A total quality approach including response to failures, and peak demand must be included, as well as resilience and other functionality measures.

These measures could be monitored by the transparency metrics required above for ensuring there is no discrimination in the delivery of service between the quality provided for an operator's own services, and that provided to its competitors. An independent body, such as an NRA, should undertake monitoring.

Question 13: In the case where NRAs find it necessary to intervene to impose minimum quality of service requirements, what form should they take, and to what extent should there be co-operation between NRAs to arrive at a common approach?

INTUG Response: Common metrics should be defined by the Commission and endorsed by BEREC in consultation with customers, and published openly. There should be proactive co-operation between NRAs to arrive at a common approach.

Question 14: What should transparency for consumers consist of? Should the standards currently applied be further improved?

INTUG Response: Transparency should produce openly available, comparable performance statistics, provided by network operators for the services they self provide, and those they deliver to other service providers. The standards currently applied need to be improved by new measures beyond the headline speeds usually quoted and compared for relative performance. There is a lack of fully comparable price/performance indicators, partly due to the prevalence of bundling, triple play and flat rate caps, although OECD is trying to address this rather complex issue.

Question 15: Besides the traffic management issues discussed above, are there any other concerns affecting freedom of expression, media pluralism and cultural diversity on the Internet? If so, what further measures would be needed to safeguard those values?

INTUG Response: The protection of freedom of expression, media pluralism and cultural diversity is outside INTUG's normal scope in representing business users. INTUG Members are aware that some parts of the world outside the EU do control access to Internet content, for non-technical reasons.

Within the EU, it is important that traffic management is exercised only for the legitimate reasons described in this response. INTUG supports policies which reduce the social and economic damage from restricted access to the Internet.

If there are differing policies within the EU, BEREC could usefully explore the possibility of introducing measures to safeguard the areas of greatest concern.

Confidentiality and Contact information

Nothing in this submission is confidential and the contents can be considered to be in the public domain. The submission is available on the INTUG web site at http://intug.org. This submission should be read in conjunction with INTUG's response to the consultation on the Next Generation Access Recommendation. The contents of that submission have not been repeated here. An INTUG press statement accompanies this response.

Comments should be addressed to:

Nick White, Executive Vice President
International Telecommunications Users Group (INTUG)
nick.white@intug.org
Tel: +44 20 8647 4858 Mobile: +44 77 1009 7638