Network Neutrality for Business Users

(safeguarding business continuity and non-discrimination)

Nick White, Executive Vice President,
International Telecommunications Users Group
(INTUG)
Heidestein 7, 3971 ND, Driebergen, Netherlands
nick.white@intug.org

***Abstract*—This paper highlights the vital importance of network neutrality and business continuity for enterprise customers in the public and private sector, and the serious risks to business users arising from application of inappropriate regulatory remedies in the event of persistent illegal file sharing and downloading.**

Keywords: end-to-end, connectivity, business continuity, open access, international, competition

I. INTRODUCTION

Future economic growth and social inclusion will depend significantly on access to the Internet and ubiquitous use of content, applications, services and devices. It will also depend on openly available and competitively supplied fibre-based broadband networks and related services. But above all, it will require adoption and implementation of the principles of network neutrality for business users of communications.

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 includes all devices, connecting services, management tools, content, applications and other elements of the ICT landscape.

Absolute neutrality is 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 eliminate, or mitigate, impact on existing investments.

II. NEUTRALITY IN BUSINESS

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 impact on past, current, or future choices for similar elements in a different place, or for a different purpose, or on any other elements that must interwork with it.

The key objective is seamless, timeless interoperability.

This extends to, but is not limited to: functionality, operability, total service quality, information content, display capability, or any other characteristic of the connected technologies being used.

Indirect connection refers to a piece of technology which is connected further away, via one or more intermediate devices, which must also not have its capabilities affected by the choice of a piece of technology anywhere in the connection chain.

III. DIFFERENTIATION, DISCRIMINATION, TRANSPARENCY

These fundamental functional issues underpin assessment of user requirements, and apply to public and private sector enterprises, SMEs and mass-market end consumers. They drive the overriding user issues concerning network neutrality, which are differentiation, discrimination and transparency. Specifically, the key questions to be answered 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 defined above be, and how visible will the consequent 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?

IV. PUBLIC AND PRIVATE ENTERPRISE NEEDS

It is vital to give full recognition to the different and distinct needs of private and public enterprise customers, compared to those of the mass-market domestic consumer. The assessment of whether or not a problem exists must not be confined only to market analysis of individual site connections by National Regulatory Authorities (NRAs) at country level.

The multi-site, multinational connectivity requirements of enterprises demand a greater level of network 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 processes 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.

V. THE RISKS OF TRAFFIC MANAGEMENT

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 (e.g. for officials and dignitaries during an Olympic Games), and traffic calming measures are implemented through speed bumps and chicanes. Fuses disconnect equipment to protect overload in electrical systems. These transparent processes are implemented visibly.

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. Yet this kind of non-neutrality exists on the Internet today. Blocking of certain applications and content cannot be justified, unless it is demonstrable that these can be classified by type of application or content, and not by the supplier or service provider.

The key is an agreed definition and classification system for applications, content and devices, which is applied consistently in all countries. This would not group together all peer-to-peer applications and block them all, when only some threaten critical latency or service integrity. This safeguard is needed if traffic management is to be used acceptably, without becoming anti-competitive discrimination.

Discriminatory non-neutrality must not be allowed either by disguising it as operational traffic management in situations of transient technical overload, emergency or security breach. The rules used for traffic management by an operator should be transparent and disclosed to users.

Traffic management is essential where there is inadequate bandwidth to cope with demand or congestion, especially in the backhaul and local loop. Other traffic management is 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 offering layered Quality of Service.

VI. NETWORK MANAGEMENT INFORMATION AND TOOLS

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 and tools. Mandatory standards to be adopted, and an obligation to provide information, are a minimum requirement.

VII. TRANSPARENCY - NECESSARY BUT NOT SUFFICIENT

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. It is still 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 of service commitments.

Implementing a distinction between services offered on a "best efforts" basis and others is, by definition, not network neutral, but may be 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.

VIII. TRAFFIC PRIORITISATION TODAY

Lack of transparency in current network operations limits ability to comment specifically on the forms of prioritization currently taking place, despite plenty of anecdotal evidence.

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 countries where such applications are not blocked.

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.

IX. TOTAL SERVICE QUALITY

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 in technical jargon 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 delivery between the quality of service provided for an operator's own business activities, and that provided to its competitors.

National Regulatory Authorities (NRAs) are best placed to define standards and undertake impartial monitoring.

X. THE RISK OF IPR PROTECTION REMEDIES

One further 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 conflict with user rights of access.

This controversial issue threatened to obstruct final agreement of the European Union Regulatory Framework Review, requiring difficult compromises between the Council of Ministers, the European Commission and NRAs.

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. Immunity from being summarily disconnected or subjected to unilateral contract termination is non-negotiable if network neutrality is to be preserved for business users.

XI. NETWORK NEUTRALITY TODAY

There is a major problem, due to the fragmented and dysfunctional fixed and mobile national markets operating 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 international 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 country-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 existing competition, such as it is, in either fixed or mobile access markets. It requires consistent co-ordinated ex-ante regulation to ensure critical bottleneck resources are expanded and are not monopolised by incumbents.

XII. DISCRIMINATION AND CENSORSHIP TODAY

Current levels of fragmentation and dysfunctionality ensure that, for most enterprise customers, the present situation does not provide network neutrality. 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.

The protection of freedom of expression, media pluralism and cultural diversity is vital. Some parts of the world today do currently control access to Internet content for non-technical reasons, for example to suppress freedom of speech and/or for political or propaganda reasons. It is important that traffic management is exercised only for the legitimate reasons described above. INTUG supports policies and regulation which reduce the social and economic damage from restricted access to the Internet.

BEREC could usefully explore possibilities for introducing measures to safeguard the areas of greatest concern and for achieving consistent minimum level recommendations to protect all users from restrictions of access to content.

XIII. REGULATING FOR NEUTRALITY

If a seamless ICT is to be created effectively, regulation for network neutrality must be consistent in all countries. Infrastructure investment is encouraged if opportunities for usage are maximized. Regulatory loopholes allowing exclusivity, e.g. via co-investment or reciprocity between wholesale broadband infrastructure owners, must be closed.

Regulation must require open access on an equivalent non-discriminatory basis to competing service providers, and prevent 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.

ABOUT INTUG

The International Telecommunications Users Group (INTUG) represents the interests of public and private business users of telecommunications globally and has been active since 1974. Users 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 EU Member States, including Belgium, Denmark, France, Germany, Spain, the Netherlands, Sweden and the UK, and the multinational user group EVUA, as well as user groups in other parts of the world. Each group represents public and private sector customers of communications service providers.

Each group represents public and private sector customers of communications service providers. INTUG has a memorandum of Understanding with the Commonwealth Telecommunications Organisation (CTO).

REFERENCES

[1] Public Consultation on the Open Internet and Network Neutrality iin Europe by European Commission - INTUG Response