Response by AT&T, BT, Cable & Wireless Worldwide, Orange Business Services and Verizon
to the European Commission Public Consultation on
Specific Aspects of Transparency, Traffic Management and Switching in an Open Internet

This response to the European Commission Public Consultation on *Specific Aspects of Transparency, Traffic Management and Switching in an Open Internet* ("the Consultation"), is submitted on behalf of the following companies: AT&T, BT, Cable & Wireless Worldwide, Orange Business Services and Verizon. All our companies are engaged in the provision of pan-European and global electronic communications services to large enterprise customers, and have business activities in several EU Member States. We are not submitting answers to all EC's specific questions.

Traffic Management, Transparency and Switching – A Different Approach Required for Large Business Customers

With regard to the EC's questions related to traffic management (**Questions 3 to 11**) and Transparency and Switching (**Questions 12 to 23**), we would like to emphasise that the nature of our retail customers, large multi-national enterprises and large public sector organisations, requires a different approach from that which may be appropriate for individual consumers and SMEs.

In general, the regulation of electronic communication services has been defined taking into account the characteristics of the mass-market services provided to consumers and SMEs, i.e., generally standardised services provided under common terms and conditions, on a mass market basis, to users who may have limited technical knowledge and relative to larger business customers, less bargaining power. Against this background, mass-market end user services have been subject to certain consumer protections. However, such consumer-oriented regulation does not necessitate the application of net neutrality (NN) regulation to larger business customers. Indeed, there are good and compelling reasons for viewing the needs of consumers and SMEs, and high end business customers, differently in terms of contractual provisions and products and in applying (or not applying) net neutrality provisions for these categories.

- Different contractual provisions

The first key difference is contractual in nature. High-end business services present various specificities that differentiate them from mass-market services:

- Significantly more complex telecom services provided: multiple locations across countries, different access technologies, bundle of services, very demanding Service Level Agreements (SLAs), etc.
- Sophisticated knowledge of the technology and economic implications of telecommunications services among high-end business users.
- Fewer customers.
- Extensive bi-lateral, individually negotiated and tailored contracts.
- Professional use of the service.

Importantly, the proposed areas of consumer regulation -- required quality levels, detailed service transparency and technical characteristics, penalties for non-compliance, etc. -- are already addressed in large part through contract. Moreover, the very nature of the European business services market, and the high level of competition in Europe, gives the large business customer a high degree of control and leverage in striking the business deal it desires in a way not generally available to consumers of mass-market Internet access services.

- Different product needs

In addition to contractual provisions, high-end businesses need products and services different from the products used by consumers. Not only are the products different, but the services purchased by businesses are often differentiated services tailored to the needs of particular customers. They generally negotiate to get the service that best meets their needs with the levels of assurance that they may demand. Businesses also have an opportunity to ask any questions they may have during the negotiation, thus minimizing the needs for standardized disclosures.

Products provided to large business (enterprise-level) customers run mainly on private IP networks (PIP), which are distinct from the public Internet. PIP services ride proprietary networks and generally involve a high degree of traffic management to meet customer's demands and needs. The need for traffic management to ensure an efficient use of the network is widely recognized by all stakeholders.

When it comes to the provision of IP based services, network management concepts are critical to a network provider's ability to comply with the service levels agreed upon with the business customer, and as such, network management requires traffic shaping tools to comply with contractual obligations.

Although many corporate customers also purchase and use "Internet access", such access service is embedded in broader data communication products, generally in a

secure manner with quality of service requirements very often dictated by the business customer.

- Increased meaningful transparency: relevance for business providers?
Increased meaningful transparency is key for consumers; however, it is not necessary for high-end business services in the context of standardized disclosures.

As noted above, most corporate customers subscribe to internet services on private IP networks. The transparency element is fully satisfied through the extensive, bi-laterally negotiated contracts between the network provider and the large business customer for these PIP services. These contracts already include all the required detail on quality levels, service transparency and technical characteristics, and penalties for non-compliance; therefore, additional regulatory protections are not necessary and indeed would skew the bilateral nature of the contract negotiation.

- QoS measures
The framework provisions enable regulators to impose minimum quality of service requirements, only if competitive forces are not enough to safeguard the openness of the Internet and transparency fails. This is decidedly not the case with large business Internet services and their related agreements.

Business service providers respond to the specific demands and needs of their customers in terms of QoS and traffic management in a different way than consumer services. Consumer uses of IP networks are very different from business customers uses (i.e. download of video, film, music). A wide array of Quality of Services parameters are individually agreed with the business customer, including periodic service reports and service level agreements (SLAs) backed by contractual penalty clauses. As such, there is no need to impose further requirements.

As BEREC's QoS Guidelines BoR (12) 32 notes on page 4: "a precondition for a competitive and transparent market is that end users are fully aware of the actual terms of the services offered". In the case of business end-users, such a precondition is satisfied and therefore the scope of regulation should properly be limited to consumer end-users.

For the reasons outlined above, we believe that the NN provisions included in the revised eCommunications regulatory framework should not be construed to apply to high-end business services and products. We further believe that the relevant

provisions of the framework[1] allow for such a distinction to be made. (In this regard, the EU framework is aligned with that of the United States where the FCC Net Neutrality Order [2] specifically excludes enterprise services from its scope.) Also in the UK, the Voluntary industry code of practice on traffic management transparency for broadband services dated March 2011[3] has limited the scope to "consumers".

However, we also believe there is a risk that a lack of clarity and precision in the use of 4 terms used in several EU legislative texts (i.e., "subscribers", "users", "end-users" and "consumers") could result in an expansion of the scope of NN regulation to operators which provide services to Business customers, even though this was not intention of the drafters of the legislation. In order to avoid this, all EU NRAs need to distinguish large business customers in a consistent manner and exclude them from the application of EU Framework NN provisions. Any future EC policy or regulatory action should insist on such an outcome.

Question 6:
The use of managed services may affect the Internet access service in some cases, due to the sharing of access resources.
a) Please explain the impact of managed services on the standard Internet access service ("best effort") in terms of available bandwidth and quality of service.
b) Please explain whether it is possible to offer separate capacity for managed services and the standard Internet access service. If yes, please provide information on the circumstances (costs, technologies) of separating them.

"Best effort" is not a "principle" of the Internet. It is merely a description of the predominant level of contractual guarantee (or non-guarantee) that the networks that comprise the Internet have chosen to provide to interconnecting networks. IETF standards have for many years supported the possibility for networks to interconnect at

[1] In particular, Articles 20 (1), 21 (3) and 22(3) of the Universal Services Directive (2002/22/EC) ("the USD"), as amended by the Citizens' Rights Directive (2009/136/EC) ("the CRD"), when read in conjunction with Recitals 21 of the CRD and 49 of the USD. These recitals make clear that, while the primary aim of the contract, transparency and quality of service provisions of the revised USD is to protect consumers, the directive may also extend to protecting micro-enterprises and SMEs that contract consumer products, but only where they so request. Crucially, no mention is made of extension to high end large business users contracting for bespoke services.
[2] Federal Communications Commission, Report and Order on Preserving the Open Internet (December 23, 2010), available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf. Para 44 defines the scope of the Order's rules as any broadband Internet access service provided to the mass market, while para 45 states: "*The term* ("mass market") *does not include enterprise service offerings which are typically offered to larger organisations through customized or individually negotiated arrangements"*
[3] Available at: www.broadbanduk.org/trafficmanagementtransparency

multiple levels of QoS different from “best effort.” Further, it is not clear at this point how the market for non-best-effort interconnection will develop in the future.

However, it would be erroneous from a commercial, technical and logical viewpoint to suggest that traffic classes using prioritisation introduce an incentive to decrease the quality of the ‘best effort’ class vis-à-vis premium classes to create a willingness to pay for premium quality.” Competitive market pressures prevent any such conduct, which would quickly drive customers to switch to rival operators that offered better performance. Indeed, providers have long offered quality of service enhancements to business-class customers, and no one has suggested that they have degraded bandwidth for the best-effort Internet access platform to increase the value of their prioritised services. To the contrary, Internet access speeds keep increasing year after year across the industry; broadband providers are investing billions to increase those speeds; and they are spending millions more on advertising to compete on the basis of double- and triple-play platforms that are shared between prioritised IP traffic (IPTV and/or VoIP) and unprioritised, best effort Internet traffic. Indeed, the introduction of advanced services generally enhances the quality and capacity of best efforts traffic because the advanced services use on average only a small fraction of increased capacity installed for these services and router queuing algorithms ensure that the unused incremental bandwidth is available for use by best efforts traffic.

Question 9:
It appears that the implementation of traffic management measures requires ISPs to analyse certain information about individual data packets, for instance by deep packet inspection (DPI) techniques. Please explain which type of information needs to be read by ISPs to implement the different traffic management measures. In which layer can this information normally be found?

It is essential to keep in mind both the fact that we only provide services to large multi-national enterprises and large public sector organisations, and the nature of the individually tailor-made negotiated contracts and services tailored to the needs of our specific customers. In addition, the products provided to large businesses and large public sector organisations run mainly on private IP networks.

Against this background, the traffic management and privacy related questions are not relevant in our context. Nonetheless we would like to make the following general observations.

There is a need to clarify what is meant by the concept of "DPI". Indeed DPI covers a wide range of practices and inspection techniques. The most used form of packet inspection is limited to what is called "shallow" packet inspection based mainly on IP header information i.e. looking at HTTP headers and URL query strings.

This distinction is clearly recognised in the EDPS Opinion on privacy and net neutrality ("*When ISPs process traffic data with the sole purpose of routing the information flow from the sender to the receiver, they generally carry out limited personal data processing"*), which also concludes that "*This does not conflict with the legal requirements of data protection, privacy and confidentiality of communications*."[4]

In general, traffic management measures don't involve "DPI", shallow packet inspection and router functionalities are sufficient.

Question 10:
a) Are there any privacy risks arising from the use of DPI for traffic management purposes, and, if so, what are the implications for transparency and consumer protection?
b) Are there alternative techniques for traffic management that do not involve deep packet inspection? Please provide examples and explain your response. Please compare those alternative techniques with deep packet inspection, in particular in terms of their effectiveness, potential impact on privacy and costs for operators.

The existing privacy legal framework at EU level already provides the necessary tools to ensure appropriate levels of privacy protection both horizontally through the technology neutral Data Protection Directive (including the proposed Regulation) and the sector specific ePrivacy Directive.

This is recognised in the EDPS Opinion: "*In principle, the EDPS considers that the existing EU privacy and data protection framework, if properly interpreted, applied and enforced, would be appropriate to guarantee that the right to confidentiality is upheld and overall that the protection of the privacy and data protection of individuals is not*

[4] EDPS Opinion on net neutrality, traffic management and the protection of privacy and personal data, 7th October 2011; p 4 para 17 (see http://ec.europa.eu/bepa/european-group-ethics/docs/activities/peter_hustinx_presentation_(1)_15_rt_2011.pdf)

jeopardised. ISPs should not use such mechanisms unless they have properly applied the legal framework."[5]

In our view, there is no need to reinvent the wheel from a privacy policy perspective but rather to focus on compliance and enforcement of the existing rules.

Question 11:
Where the user's consent is required for traffic management measures, particularly where such measures might entail access to and analysis of certain personal data by ISPs, please explain how (e.g. in which format) this consent should be sought by the ISP, what prior information needs to be provided by the ISP to the user, and how the user consent should be given, in order to optimise user awareness and user convenience.

As mentioned previously, there is already an adequate privacy framework in place in the EU. More specifically, the ePrivacy Directive includes provisions for legitimate processing of traffic and communication data without the need for prior consent (articles 4 and 6). These legal grounds include delivering the service, safeguarding the security of the service and minimizing congestion.

The EDPS further highlights that: "*When ISPs process traffic data with the sole purpose of routing the information flow from the sender to the receiver, they generally carry out limited data processing*"[6].

Question 24:
a) In your view, are there any problems regarding IP interconnection arrangements (between network operators, ISPs, transit providers and/or content providers) that could have an impact on the quality of the best effort Internet?
b) Are there any specific issues related to the vertical integration of ISPs and transit providers?

We believe that the IP interconnection market is highly competitive:

- Internet traffic arrangements are negotiated in highly competitive markets,
- prices for transit services are continually declining,

[5] EDPS Opinion on net neutrality, traffic management and the protection of privacy and personal data, 7th October 2011; p 18, para 80
[6] EDPS Opinion on net neutrality, traffic management and the protection of privacy and personal data, 7th October 2011, p 4, para 17

- ISPs and content providers have many options for exchanging traffic, and
- no Internet backbone provider has market power.

We welcome the indication in BEREC's recent Draft Report on IP interconnection[7] that regulation of IP interconnection may not be justified because the Internet ecosystem has consistently demonstrated an ability to adapt to address needs and developments. Specifically, we agree with BEREC's key conclusion that "[t[he market has developed very well so far without any significant regulatory intervention."[8]

To date, no European regulatory authority has identified any market failure, or applied regulation to Internet wholesale arrangements. In its response to the European Commission's 2010 Questionnaire on Net Neutrality, BEREC supported the absence of regulatory intervention on the basis of market competitiveness: "[Peering and transit interconnection] agreements have been largely outside the scope of activity of National Regulatory Authorities (NRAs). This appeared justified in particular due to the competitiveness of the transit market on IP backbones."[9]

BEREC's Draft Report further notes (p.50) that disruptions of interconnection at the wholesale level, leading to a situation where end-users cannot reach all destinations on the Internet have been few and have to date been solved in a relatively short time without regulatory intervention – also due to competitive pressure of end-users at the retail level.

We therefore assert that their highly competitive nature means that EU Internet interconnection markets cannot satisfy the "three criteria" test for *ex ante* regulation – high and non-transitory entry barriers, the structure of the market must not tend towards effective competition, and the application of competition law alone must not be able to adequately address the market failure concerned.[10]

[7] *An Assessment of IP Interconnection in the Context of Net Neutrality*, BEREC Draft Report for Public Consultation, (BoR(12)33)
[8] *Id.* at page 50
[9] BEREC's Response to the Commission Questionnaire on Net Neutrality (BEREC(10)42);
[10] *See* Commission Recommendation of 17 December 2007 on Relevant Product and Service Markets, Art. 2, 2007/879/EC.

Question 28:

Do you consider that regulators should monitor interconnection agreements between providers?

No. Regulators can obtain a wealth of information regarding the Internet interconnection marketplace and Internet traffic arrangements by using publicly available data and reports, or by commissioning studies from competent third parties to assess whether the interconnect markets are working correctly.

15 October 2012