

To: Policy Development Unit (B1), BU33 7/40  
DG Information Society and Media  
European Commission  
B-1049 Brussels  
Belgium  
Tel +32 2 297 1622  
Email: [INFSO-NETNEUTRALITY@ec.europa.eu](mailto:INFSO-NETNEUTRALITY@ec.europa.eu)

September 2010

**Skype comments on the European Commission consultation on the open Internet and net neutrality in Europe**  
([http://ec.europa.eu/information\\_society/policy/ecomm/doc/library/public\\_consult/net\\_neutrality/nn\\_questionnaire.pdf](http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/net_neutrality/nn_questionnaire.pdf))

Skype Communications sarl (hereafter ‘Skype’, [www.skype.com](http://www.skype.com)) is a Luxembourg-based provider of peer-to-peer software applications which enable Skype users to communicate with other Skype users, and enabling, optionally and where possible, certain forms of communication with the subscribers of electronic communications networks and services.


Please find hereby Skype’s brief comments on the consultation by the European Commission on the open Internet and net neutrality in Europe.

**General remarks**

Skype welcomes the European Commission’s clear commitment to an open Internet as a prime policy objective. We strongly support the view that the Internet is now ‘*central to people’s lives... empowers citizens and brings a better quality of life ... is an engine for creating more growth and jobs... a platform for the delivery of public and private services.*’ We would suggest that this important starting point should be strongly reiterated and made clear to all national regulatory authorities around the EU as they implement this policy commitment in furtherance of the consultation’s primary aim to ‘*preserve the open and neutral character of the Internet*’.

**Summary of key points in Skype’s response**

1. End-users’ ability to access and distribute the information or run the applications and use the services of their choice on the Internet is severely limited across the European Union.
2. The traditional ex post competition approach is insufficient to redress the widespread harm to innovation, citizens and consumers already witnessed.
3. The European Commission should send strong signals to avoid the expansion of existing abuse to an even wider array of Internet content, applications and services, which would considerably devalue the social and economic utility of the Internet.
4. Two approaches are necessary to preserve the open character of the Internet:
  - (i) clear guidance by the Commission on the *ex ante* principles underpinning the protection of the open Internet in the revised Electronic Communication Framework, including:
    - a. a definition of Internet access (as meaning access to the whole of the public, open Internet) being clearly distinct from managed services;

- 
- b. the recommendation that all end-users should be able to have a minimum QoS access to the best efforts Internet whichever other services they subscribe to, for both fixed and mobile access, and that what constitutes such functional Internet access be assessed regularly so as to avoid the Internet becoming an under-invested 'dirt road', or, conversely, being affordable only to the richer segments of the population; and
  - c. specifying the scope of reasonable traffic management as exceptional, relevant, proportional, efficient, transparent and non-discriminatory.

(ii) unequivocal duties and powers for NRAs to enforce the protection of these open Internet principles, e.g. with the ex ante imposition of the provision by each and every network operator of access to the best efforts Internet.

5. The revised EU Framework clarifies that measures restricting end-user access must be "*appropriate, proportionate and necessary*". The Commission should expand this, drawing from best practice such as ARCEP's to state unequivocally that "*the traffic management practices that ISPs employ to ensure Internet access [should] remain exceptional and comply with the general principles of relevance, proportionality, efficiency, transparency and non discrimination*" and that it is not legitimate to block or otherwise hinder any services and applications.
6. Relying solely on transparency would create a *de facto* loophole for operators to practice restrictions of their own volition as long as they inform consumers, as already evidenced in Sweden this year.
7. The Commission should make it clear that not including access to the global public Internet in broadband access offers would be an unwelcome step backwards; that limitations to end-users' 'Internet access' should only concern speeds or volume caps; and that having "access to the Internet" should clearly mean access to all of the Internet, rather than a subset of it.
8. The main risk of harm when it comes to prioritization lies with the 'last mile' and possibly the backhaul segment. We see no particular problem in an operator offering both access to the Internet and other services; however, provision of best efforts (open) Internet access should not be unduly and arbitrarily degraded, or its capacity rationed, to the benefit of the operator's own or affiliated services.
9. When it comes to managed services, if the operator were to offer to prioritise certain content, application or service, it should be on a fair and reasonable (FRAND) basis.
10. The Commission should make it clear that it would be neither desirable in any case, nor timely, to give 'carte blanche' to network operators to start charging online businesses for traffic delivery or origination.
11. Safeguarding the open Internet is central to the respect of fundamental freedoms online and to ensuring continued benefits for all in the value chain, starting with consumers, and including continued innovation and (return on) investments in infrastructure.



## Specific remarks on the Commission's Questions

***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?***

End-users' ability to access and distribute the information or run the applications and use the services of their choice on the Internet is severely limited across the European Union, despite this ability being highlighted as a policy principle and objective by the European legislator in the revised Framework Directive on Electronic Communications (Article 8.4(g)). This state of affairs is due in particular to arbitrary discrimination imposed by mobile network operators on the use of specific Internet content, applications and services. Indeed, many mobile network operators, including all GSM/UMTS operators in several EU Member States, have decided to adopt technical and/or contractual conditions preventing users from using VoIP and P2P applications, and certain other forms of utilisation are otherwise impeded or subject to unjustified additional retail tariffs, such as video, audio, tethering, streaming or newsgroups.

The problem is therefore centered on the Internet access bottleneck, and is particularly relevant in mobile markets, where only a limited number of providers exists (in many European markets, there are only 3 to 5 mobile network operators, and the top two MNOs typically have 75-90% combined market share). In spite of the existence of multiple independent underlying infrastructures, the mobile retail market exhibits characteristics that do not reflect an effectively competitive market, and often fails to offer consumers a meaningful choice.<sup>1</sup> Additionally, when users subscribe to a long-term mobile telephony contract, their provider is the *de facto* monopoly provider of mobile Internet access for the duration of the contract – i.e. they have bottleneck control over users' Internet access.

This means that the traditional *ex post* competition approach is usually powerless to redress the widespread harm to innovation, citizens and consumers already witnessed around the EU: operators without significant market power are as likely as those with SMP to engage in harmful discrimination; mobile retail markets are excluded from market reviews in Member States and hence escape close scrutiny by NRAs; and competition cases are also long affairs, often taking up to 10 years, which are also very costly and therefore simply impossible to carry out for most European companies evolving in the Internet layer (more than 95% of EU ICT firms are SMEs).


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

---

<sup>1</sup> Restrictions to end-users' ability to access and distribute the information or run the applications and use the services of their choice on the Internet are widespread across the EU. For example:

- In the UK, wide-ranging restrictions are in place for mobile access to the Internet, ranging from the ban of the use of VoIP, P2P, audio, video, or streaming, to the surcharging of VoIP use.
- In France, all three mobile operators have prohibitions in place concerning the use of VoIP, peer-to-peer and newsgroups, including for the new iPad.
- In Sweden, the two leading mobile operators have introduced bans on VoIP in 2010 (see response to question 5 for details).
- Limitations on the use of VoIP, P2P and other applications on mobile are also prevalent in Germany, Italy, the Netherlands, Spain, UK and other EU countries.

We don't have sufficient resources to check all 27 EU markets for similar restrictions.



We see widespread abuse already taking place in the current market environment such as the arbitrary blocking and degradation of traffic. It is crucial that European authorities send a very clear signal – through pro-active and urgent enforcement – of their commitment to the objective and principle of an open and neutral Internet. In the next generation environment, market consolidation is likely and the number of providers in a position to invest in next generation access infrastructure may be limited. It will be important to acknowledge the potential for future market structures to incentivise discriminatory behaviour, particularly the abuse of bottleneck control over users’ Internet access. Further, the fast-moving vertical and horizontal integrations and commercial dynamics within the converged Internet / ICT ecosystem (from hardware, to operating systems, to networks, to content, etc.), exemplified by such phenomena as ‘bundling’, could accelerate the trend towards undesirable discriminatory practices that would have negative consequences for innovation, consumer choice, trade, etc.

Without strong signals by the European Commission and other European authorities, it is likely that many network operators will feel justified or condoned in their practices and feel comfortable extending their abusive restrictions to cover an even wider array of Internet content, applications and services. The Internet will become a number of subsets driven by commercial partnerships that will considerably devalue the social and economic utility of the Internet (restricting new / innovative products and services, not maximising value for the ICT value chain and for users and society as a whole).

At this stage, we would urge the authorities to focus their actions on solving problems at the Internet access layer where abuses are witnessed now, whilst monitoring in parallel developments in other layers of the value chain and be ready to act there too as may be required. In the longer term, the European authorities and policymakers generally may want to engage in a reflection on how competition law can be more flexibly applied so as to counter various types of abuse.

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


In our view, and as already suggested by the European Commission<sup>2</sup>, limitations to end-users’ ‘Internet access’ should only concern speeds or volume caps. Having “access to the Internet” should clearly mean access to all of the Internet, rather than a subset of it. The only exceptions, apart from legal restrictions on illicit uses of the Internet, should be for traffic management purposes from a purely technical perspective to improve end-user experience in temporary cases of acute congestion, and so as to preserve the security and integrity of networks.

As mentioned in response to question 1, ex post competition law is likely to be insufficient to deal with these issues, but the electronic communications framework provides a good basis. Accordingly, we believe that two approaches are necessary:

- (i) The European Commission should issue clear guidance on the *ex ante* principles underpinning the protection of the open Internet in the revised Electronic Communication Framework, including what constitutes reasonable traffic management.
- (ii) The revised Framework should be judiciously implemented in national laws so as to give unequivocal powers for National Regulatory Authorities to enforce the protection of open Internet

---

<sup>2</sup> See European Commission statement on the telecom package, <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/219&format=HTML&aged=0&language=EN&guiLanguage=en>



principles. This could take the form in particular of the ex ante imposition of the provision by each and every network operator of access to the best efforts Internet, so as to *prevent* abuse, as outlined in Article 22.3 of the Citizens' Rights Directive. (we detail below in response to questions 9 and 11-13 how this should be developed, reviewed and enforced)

***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?***

Traffic management is sometimes a necessity in today's Internet infrastructural environment, for example in certain cases at times of peak usage where network efficiency must be maximized to avoid undue congestion and slowing of network traffic. Nevertheless, traffic management techniques should be deployed only on an exceptional, needs-only basis.

Considering the importance rightly placed by European governments and the European Commission, for instance in the *Digital Agenda for Europe*, on fostering the rollout and take-up of the broadband Internet by all Europeans, it is important that traffic management techniques are not allowed to be used as a substitute for an increase in capacity whenever possible. The authorities should avoid the best efforts Internet becoming a low speed, low capacity 'dirt road' by deliberate choice of network operators or through lack of investment. Adding capacity in line with the overarching objective of promoting the continued development of the Internet must remain the preferred solution.

Secondly, the revised EU Framework for Electronic Communications already clarifies that measures restricting end-user access must be "*appropriate, proportionate and necessary*"<sup>3</sup>. Skype suggests that the European Commission could usefully expand on these qualifications by issuing guidance that would scope what is deemed reasonable traffic management. This would give regulatory certainty and enable operators to manage traffic flexibly where necessary on an exceptional basis, whilst ensuring that such management does not harm end-users, competition or innovation.


We point the European Commission in this respect to emerging regulatory best practice.

The Canadian regulator CRTC provided a blueprint for scoping acceptable traffic management practices<sup>4</sup>, and in Europe the French regulator ARCEP has already provided some good directions.

---

<sup>3</sup> Article 1.3, Framework Directive 2009/140/EC.

<sup>4</sup> When concern arises over traffic management practices, the CRTC recommends that ISPs should be able to demonstrate in particular "*the need for [Internet Traffic Management] and its purpose and effect, and identify whether or not the ITMP results in discrimination or preference; [...] In the case of an ITMP [Internet Traffic Management Practice] that results in any degree of discrimination or preference: demonstrate that the ITMP is designed to address the need and achieve the purpose and effect in question, and nothing else; establish that the ITMP results in discrimination or preference as little as reasonably possible; demonstrate that any harm to a secondary ISP, end-user, or any other person is as little as reasonably possible; and explain why, in the case of a technical ITMP, network investment or economic approaches alone would not reasonably address the need and effectively achieve the same purpose as the ITMP.*" CRTC Telecom Regulatory Policy CRTC 2009-657, *Review of the Internet traffic management practices of Internet service providers*, October 21, 2009, <http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm> and <http://www.crtc.gc.ca/eng/archive/2010/2010-445.htm>



ARCEP scoped the appropriateness of traffic management as follows: "[ARCEP] recommends that the traffic management practices that ISPs employ to ensure Internet access remain exceptional and comply with the general principles of **relevance, proportionality, efficiency, transparency and non discrimination**"<sup>5</sup>. The details it gives on each qualification are also very helpful to scope what practices are acceptable. In particular, 'non-discriminatory' "means that streams with comparable technical properties must be treated in an equivalent fashion. The particular goal is to prevent an ISP from favouring its partners' content/services/applications (or its own if it is vertically integrated) over those supplied by others, as this type of preferential treatment must be reserved for managed services only, and cannot apply to Internet access."<sup>6</sup>

We would also add that beyond considerations solely related to traffic management, arbitrary discrimination against certain applications and protocols should not be deemed legitimate. As ARCEP noted, "within specific technological environments, and particularly on mobile networks, although the overall goal must prevail, it nonetheless seems acceptable for mobile operators to restrict access to certain sites or applications for objective, non-discriminatory and justified reasons [...] this type of constricting practice must nevertheless only be possible when it satisfies real technical imperatives, and can never involve banning or blocking an application or a protocol (including voice over IP, peer-to-peer or streaming), nor must it act as a substitute for investing in increasing network capacity, which is the solution that must prevail in the medium term." On VoIP specifically, ARCEP added that "even in data offers that are not qualified as "Internet access," it does not seem legitimate to block voice over IP services (such as Skype) since that they not consume more bandwidth than other services that are currently accessible via mobile networks."<sup>7</sup> We would concur of course, and wish to point to a common misconception: VoIP or peer-to-peer applications are not inherently bandwidth-hungry. A typical Skype voice call, for example, consumes only between 6 and 20 Kbps, which is the equivalent of downloading a normal webpage. It is therefore clear that the sort of blanket discrimination of certain protocols and types of applications like VoIP or P2P is wholly misleading and illegitimate. We encourage the Commission to make this point clearly, as ARCEP has done.

In this respect, we would also remind the Commission that removing such barriers to the development of VoIP is mandated under the EU Roaming Regulation, as amended in 2009, which stipulates that "[...] there should be no obstacles to the emergence of applications or technologies [...] such as WiFi, Voice over Internet Protocol (VoIP) and Instant Messaging services."<sup>8</sup>

**SEE ANNEX 1 for details on the traffic management techniques that can be deployed for blocking and degradation.**


**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 on the one hand and services offering access to the public internet on a 'best efforts' basis, on the other?**

<sup>5</sup> ARCEP consultation *Discussion points and initial policy directions on Internet and network neutrality*, May 2010, English version; [http://www.arcep.fr/uploads/tx\\_gspublication/consult-net-neutralite-200510-ENG.pdf](http://www.arcep.fr/uploads/tx_gspublication/consult-net-neutralite-200510-ENG.pdf).

<sup>6</sup> ARCEP, *Ibid*, page 18.

<sup>7</sup> ARCEP, *Ibid*, pages 33 and 19.

<sup>8</sup> Article 40. The full text of the regulation can be found here: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:167:0012:0023:EN:PDF>



Transparent information informing users about limitations placed on their access service is always welcome, but we have reservations about the effectiveness of transparency provisions in this context.

Proposals which rely solely on transparency are not only insufficient, but they could have the opposite effect of what they are aimed at (promoting the open Internet), by creating a *de facto* loophole for operators to practice restrictions of their own volition as long as they inform consumers.

We see a clear risk that this could lead to a situation wherein all ISPs are in a sense encouraged to tier their offers to provide comparable subsets, and whereby unrestricted Internet (without subsets) becomes de-facto the highest tier/most expensive option. Clearly, this should be actively avoided. We call on the Commission and on other involved authorities to keep this risk prominently in mind.


We are already witnessing the perverse effects of a sole reliance on transparency provisions in Sweden for example: until last year all mobile network operators offered access to the full, unrestricted Internet. But since the beginning of this year when regulator PTS pronounced itself in favour of transparency as the only safeguard for the open Internet, both leading mobile operators introduced restrictions on users' ability to use VoIP<sup>9</sup>.

The situation is compounded by the continuing and severe challenges encountered by European consumers in switching providers. Examples include early termination fees, handset exclusivity practices, bundling of handsets and service contracts, non-portability of email addresses and web hosting space supplied by and tied to the operator, residual number porting issues, etc. Given the cost and the time and effort involved in switching a consumer may (even if aware of the initial restrictions they are affected by) decide that the switching costs exceed the loss in utility of the closed network. Nevertheless, the loss in utility remains — to say nothing of the crippling effect such individual actions have on the market for innovative third-party applications, services, and devices.

The difficulty in switching was evidenced already for example in the UK (reputedly one of the more competitive markets in the EU) by Ofcom having had to intervene in 2007 with a new regulation to facilitate customers being able to switch providers easily (*Ofcom General Condition 22: Service Migrations*), and there are still significant deficiencies: Ofcom's *Consumer Experience Report 2009* further reported that switching by both household and business consumers in the mobile, fixed, and Internet sectors was far lower than in many other sectors such as electricity, gas or car insurance. Ofcom published research as recently as 10<sup>th</sup> September 2010, which showed that “nearly half (45%) of consumers with broadband or a landline think that switching communications provider is too much hassle”<sup>10</sup>.

<sup>9</sup> See Telia Sonera's and Telenor's Terms and Conditions here : [https://www.tewss.telia.se/privat/produkter\\_tjanster/mobilt/surfaimobilen/?sl=privat\\_produkter\\_tjanster\\_mobilt\\_surfaimobilen](https://www.tewss.telia.se/privat/produkter_tjanster/mobilt/surfaimobilen/?sl=privat_produkter_tjanster_mobilt_surfaimobilen) and <http://www.telenor.se/privat/abonnemang/tillaggstjanster/alla-mobiltjanster.html#C45-2100-P45-5468>.

<sup>10</sup> Ofcom press release: “Nearly half of consumers put off by switching communications provider”( <http://media.ofcom.org.uk/2010/09/10/nearly-half-of-consumers-put-off-by-switching-communications-provider-2/>), ‘Consumer Switching and Bundling’, Research for Ofcom prepared by Saville Rossiter-Base (<http://stakeholders.ofcom.org.uk/binaries/consultations/consumer-switching/annexes/switching-bundling.pdf>) and ‘Consumer switching: Experimental economics research’, Research for Ofcom prepared by London Economics (<http://stakeholders.ofcom.org.uk/binaries/consultations/consumer-switching/annexes/economics-research.pdf>), both published on 10 September 2010.



The European Regulators' Group / BEREC has also been forced to continue its working group on switching for yet another session due to the persistent consumer harm faced in this area.

For these reasons Skype believes that the Commission should protect the open Internet by: making it clear (in forthcoming guidance suggested in response to question 3) that

- not including access to the global public Internet in broadband access offers would be an unwelcome step backwards;
- having "access to the Internet" should clearly mean access to all of the Internet, rather than a subset of it;
- limitations to end-users' 'Internet access' should only concern download speeds or volume caps (as clarified by the Commission in 2009<sup>11</sup>); and that
- transparency concerning limitations to end-users' access should not be mistaken for a loophole enabling by-the-backdoor discrimination of specific services, applications, technologies, sources or destinations, except for genuine legal or technical reasons.

Further, in implementing the revised Framework, national legislation should provide for a duty and unequivocal power for NRAs to enforce open Internet principles.

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

EU regulations are rightly technology-neutral. There is no justification for any difference between open Internet rules that would be applied to fixed or wireless. In applying open Internet safeguards, regulators will, where appropriate, make the necessary distinction in technical specificities between mobile and fixed when they monitor the market and/or when a case where harm is caused is initiated.

It is widely predicted that one billion subscribers will access the Internet through mobile devices by 2013 - as many as through fixed access.<sup>12</sup> If the open Internet is not allowed to thrive in the mobile world, its utility to European citizens, society and the wider economy would be tremendously diminished.


***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 prioritization affect other players in the value chain?***

It is well known that measures can be taken high up in the Internet architecture so as to enable content to be available more rapidly and with more reliability to end-users. An example is the use of Content Delivery Networks (CDNs) that can transport IP traffic through dedicated routes and store / cache it closer to the end-user – as close to the last mile as possible. These methods are, importantly, open to any Internet content, service or application provider, in competitive conditions. We are not aware or concerned that these methods cause harm to online providers or end-users.

---

<sup>11</sup> European Commission statement on the telecom package, <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/219&format=HTML&aged=0&language=EN&guiLanguage=en>

<sup>12</sup> Morgan Stanley's Mary Meeker, 'Economy + Internet trends', October 20, 2009, [http://www.morganstanley.com/institutional/techresearch/pdfs/MS\\_Economy\\_Internet\\_Trends\\_102009\\_FINAL.pdf](http://www.morganstanley.com/institutional/techresearch/pdfs/MS_Economy_Internet_Trends_102009_FINAL.pdf)



The main risk of harm when it comes to prioritization would lie instead with the ‘last mile’ and possibly the backhaul segment where the end-user’s network operator has bottleneck control over users’ Internet access and can therefore dictate the conditions of both the delivery and the origination of traffic. This is a particularly salient and real threat of harm, notwithstanding the perceived market power of an ISP, since as explained in the draft TERA study<sup>13</sup> for the European Commission “An Internet user never receives calls:

*To use the example of a famous video sharing platform, it is always the user who “calls” YouTube, never the contrary. It could be argued therefore that the Internet access provider applies a Calling Party Pays regime in its relations with the Internet user. As the “calling party”, the Internet user bears the full cost of the communication on the access network.”*

Although we see no particular problem in an operator offering both access to the Internet and other services, provision of best efforts (open) Internet access should not be unduly and arbitrarily degraded, or its capacity rationed, to the benefit of the operator’s own or affiliated services.

***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 which are in the same situation? May exclusive agreements between network operators and content/application/online service providers create problems for achieving that objective?***


The European Commission should define clearly what is meant by ‘managed services’ and separate it from the definition of ‘Internet’. The type of definition proposed by ARCEP is helpful in this respect. ARCEP separated the best efforts, open and public Internet from the private networks that are used to provide managed services. This distinction is important both to avoid end-user / consumer confusion and to protect the open Internet as a unique global platform for innovation and the free flow of information.

We encourage the Commission to define and distinguish Internet access and managed services along the following lines, inspired by ARCEP’s proposals<sup>14</sup>:

- “Internet access: *a service that consists of providing the public with access to online communication and information services and applications*<sup>4</sup>. *This service provides the public with the ability to send and receive data by using the IP communication protocol, from all or virtually all points from all of the interconnected public and private networks around the world that make up the Internet.* “
  
- “Managed services: *services providing access to content/services/applications through electronic means, marketed by the network operator which guarantees certain specific features thanks to the process it uses on the network it owns and operates. Some of the classic features include guaranteed reliability rate, minimal latency, jitter (variation in time between packets), guaranteed endpoint-to-endpoint bandwidth, security level, etc. According to the above definition, providing end users with access to the Internet does therefore not constitute a managed service. Some managed services can be governed by a contract with an ISV, and may also result from an offer made available to the end user, whether as a standalone offer or in the form of an option bundled with Internet access.*”

<sup>13</sup> ‘Study on the future of Interconnection methods’, Tera Consultants for the European Commission, Section 3.1.2.2.4, page 36 <http://www.teraconsultants.fr/assets/publications/PDF/2009-70-MR-draft-final-study%28consult%29.pdf>.

<sup>14</sup> ARCEP, *Ibid*, Pages 7-9. ARCEP refers to content, applications and services providers as ‘Information Society Service Vendors’ or ‘ISVs’



When it comes to managed services, were the operator to offer to prioritise certain Internet content, application or service, it should be on a fair and reasonable (FRAND) basis. Questions around the fairness and reasonableness of any exclusivity arrangements could be dealt with as they are today through competition and/or commercial law.

**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?**

The European Commission should issue, and regularly review, guidance – or issue a regulation – including a definition of Internet access (as meaning access to the whole of the public, open Internet) vs managed services; the recommendation that all end-users should be able to have a minimum QoS access to the best efforts Internet whichever other services they subscribe to; and specifying the scope of reasonable traffic management. This guidance should also include that all services should be provided on a fair and reasonable (FRAND) basis.

To ensure that this guidance is adhered to, the Commission should be ready to enforce, and should commit to monitor developments in the market, report regularly and publicly to the EU institutions, and be ready to act by using, inter alia, measures from Art 22.3 of the Citizens' Rights Directive, including around managed services, should there be a clear and imminent (or existing) threat of harm to consumers / end-users, innovation, or competition.

**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?**


The current arrangements that govern the Internet work well. Any content, application or service can be put online without the need to ask (operators or anyone else) for permission. This successful model has been built upon the basic principle of non-discrimination. It has allowed innovative content, products, applications and services and information of all kinds to appear and be disseminated on the Internet without the need to seek prior permission from anyone. It underpinned the unprecedented wave of innovation, worldwide interactions and competition across numerous sectors and societies. It contributed to a more than 40% increase in productivity over the last decade in the European Union. This virtuous cycle of online innovation in turn generated renewed end-user demand for Internet access, itself providing return for investment in networks.

Disturbing the fundamental 'rule of the game' behind the Internet economy's success that is the open and neutral character of the Internet would have serious and negative consequences far beyond the ICT value chain. This was reiterated by the European Parliament as recently as 21 September 2010, stressing "*the importance of open and neutral access to a high-speed internet connection, without which e-commerce would be impossible*".<sup>15</sup>

Providers of online services and applications – from pure Internet companies to the banking or travel sector through to public institutions – make investment decisions on the understanding that

---

<sup>15</sup> Report on completing the internal market for e-commerce A-7-0226/2010, <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2010-0226&language=EN&mode=XML>, or <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2010-0226+0+DOC+PDF+V0//EN>



their product or service is potentially discoverable by any Internet user. They make projections, investment, research & development, and marketing decisions on this basis. If access infrastructure and the way in which it is managed impacts on potential audience / customer base size and reach, it will also impact revenue for downstream businesses. Were a third party able to exercise a level of control over the actual size of the audience or customer base, a website owner or application provider would not have the same degree of confidence. This would immediately compromise the business case of numerous prospective start-ups, creating a tax on innovation and entrepreneurship.

Morgan Stanley predicts a mobile Internet market of more than one billion subscribers by 2013.<sup>16</sup> The GSMA forecasts that within the next 15 years there will be more than 50 billion mobile connections thanks to the 'Internet of Things'<sup>17</sup>. The suggestion made by some to oblige those content and applications providers who ensure that consumers continue to see value in paying operators for Internet access to additionally pay the same operators for delivering (or originating access to) their content and applications traffic to consumers is a warped logic: no consumer wants a fiber optic cable to arrive at their house, or a satellite dish to be attached to their roof – the hardware is a means to an end. The end-goal is to access the Internet content, applications and services of their choice. Operators who attempt to make it more difficult for the Wikipedias, the Facebooks, the Skypes, and the many start-up guys in their garages to innovate online are also harming themselves by reducing the flow of innovation which drives demand for Internet access.

For all these reasons, it would be neither desirable nor timely to give 'carte blanche' to network operators to start charging online businesses for traffic delivery or origination. A tax on innovation would be unwelcome at the best of times. In the current difficult economic environment, it would run counter to efforts at re-engineering economic growth in the EU and elsewhere.

***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?***


The goal of the revised European legislators, as unambiguously worded in Article 22.3 of the Citizens' Rights Directive (see our response to question 3), is to empower NRAs to impose a minimum quality of service to *prevent* blocking or degradation of service.

So as to conform to this clear direction, and considering that blocking, degradation and other hindrances to services and content that consumers want to access are already widespread and hence require intervention, Skype believes that ex ante minimum quality of service levels should be imposed, whereby, **an end-user should always be able to access the best efforts, global public Internet, whichever other / managed services they may also be subscribing to.** This would enable operators to innovate in their offerings, whilst ensuring that end-users are always able to enjoy all Internet content, applications and services whichever operator or package they subscribe to. The only exception, as we have already described, should be reasonable traffic management

---

<sup>16</sup> ['Mary Meeker: Mobile Internet Will Soon Overtake Fixed Internet'](http://gigaom.com/2010/04/12/mary-meeker-mobile-internet-will-soon-overtake-fixed-internet/), 12 April 2010 (<http://gigaom.com/2010/04/12/mary-meeker-mobile-internet-will-soon-overtake-fixed-internet/>) and 'Economy + Internet Trends', Morgan Stanley / Mary Meeker, 20 October 2009 ([http://www.morganstanley.com/institutional/techresearch/pdfs/MS\\_Economy\\_Internet\\_Trends\\_102009\\_FI\\_NAL.pdf](http://www.morganstanley.com/institutional/techresearch/pdfs/MS_Economy_Internet_Trends_102009_FI_NAL.pdf))

<sup>17</sup> <http://www.telecoms.com/17954/2020-vision-the-decade-ahead/>



In defining what a minimum quality of service level for the best efforts Internet would constitute, taking into account as necessary such aspects as connection speed, jitter and latency requirements, we encourage the European Commission to engage in further work in this area, involving all relevant stakeholders in the process, referring to the European legislation which specifies ‘functional Internet access’ to be available to all Europeans. Accordingly, we also encourage the Commission to liaise with national regulatory authorities, such as ARCEP, who are also engaged in similar work at this point in time.

It is also important, as mentioned above, that in forthcoming Commission guidance and in defining a minimum quality of service level, it is made clear that: (i) network operators should be encouraged to continue to invest in improving the infrastructure underlying the best efforts Internet, and not just the infrastructure underlying the managed services they may also provide, and (ii) that access to the full Internet should not become over-priced compared to managed services, that the Internet becomes a utility available only to the richest segments of the population. This would ensure that the Internet does not become a ‘dirt road’, a clear risk to diminish the social and economic value of the Internet. In the future, European and national authorities should accordingly impose minimum quality of service requirements if / when Internet speeds, which have increased systematically over time, cease doing so.

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

***AND***

***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?***


See our answer to question 9. In addition to the application of clear and meaningful transparency provisions to consumers, to help ensure that its guidance on protecting the open Internet is adhered to, the Commission should be ready to take enforcement action. It should further commit to monitor developments in the market, report regularly and publicly to the EU institutions, and be ready to act by using, inter alia, *ex ante* measures from Art 22.3 of the Citizens’ Rights Directive, including around managed services, should there be a clear and imminent threat of harm to consumers / end-users, innovation, or competition.

We encourage the European Commission and NRAs to set up multi-stakeholder working groups to define which minimum quality of service level is appropriate to enable any European Internet user to have ‘functional Internet access’. Some work in this area is already being proposed, for instance by ARCEP, and although certain conditions will differ depending on each member state’s particular level of Internet access development, some coordination and exchange of best practices should be encouraged, notably through and with the involvement of both BEREC and the European Commission.

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

As mentioned above, end-users should be clearly informed whether what they are buying is Internet access or not. Anything that is not the whole of the Internet cannot be described as the Internet. Misleading descriptors such as “web access”, “surfing the web”, “the best of the Internet” or “3G access” should also be strongly discouraged.





Clarity could take the form of short and simple ‘key facts’ understandable by the “man in the street” made available next to more detailed, including technical, information. Examples such as the UK Financial Services Authority’s practice could be highlighted here: when buying a financial product, consumers are presented with both a simple, usually one-page-long ‘Key Facts Illustration’ with easy to understand main details of the offering, followed by an in-depth brochure detailing the terms and conditions. This would enable consumer alpha to understand what access they are buying (how much bandwidth they can consume, how much speed they can expect etc. as well as any other substantial restrictions) so that they can compare it easily with other offers, and also for both consumers and other end-users such as online companies to find out more about the detail on specific points by going to the longer section if necessary, for instance to verify how traffic management techniques are deployed.

***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?***

It is clear that restricting arbitrarily certain uses of the Internet has serious consequences for citizens’ rights. Taking an example close to us, someone should be able to speak to and/or see their family using Skype if they want to, once they have paid for Internet access. Operators should not have the right to dictate when, how or whether citizens can communicate with their friends and loved ones, or, indeed, with anyone.


Media pluralism and cultural diversity are at risk in a world of several possible clustered, closed subsets of the Internet, where content can be accessed only if included in a commercial deal between the operator and a particular content provider. The global wealth of knowledge available through the Internet would be directly affected by threats to the open Internet. The emergence of bundled services and exclusive media and content deals could have serious consequences in this respect.

As Jack Balkin, Knight Professor of Constitutional Law and the First Amendment at Yale Law School, put it:

*“The infrastructure of free expression includes the kinds of media and institutions for knowledge, creation, and dissemination that are available at any point in time. It also concerns the kinds of opportunities that are available for people to create and build technologies and institutions that other people can use for communication and association. Two contemporary examples are Internet telephony and file-sharing services like BitTorrent. These new applications—which allow people to communicate and trade information and files cheaply—were possible because entrepreneurs could lay new applications on top of Internet protocols. People could create these new applications because the structure of the Internet allowed this sort of experimentation without getting anyone else’s permission in advance. By choosing a regulatory scheme that lets the Internet function more or less as a general data transport system, we open up possibilities for a wide variety of new applications and services that can let people share information and opinions, build things together, and form online communities.*

*[...] Policies that facilitate this kind of innovation—and that allow many people, not just network providers, to engage in it—better serve the interests of freedom of speech in the long run.[...] Yet the larger question in the debate over network neutrality is innovation policy. That question has enormous implications for media access and for future opportunities to speak, listen, share information, and associate with others.”<sup>18</sup>*

<sup>18</sup> Jack M. Balkin, ‘The Future of Free Expression in a Digital Age’,



There is a further threat in condoning restrictions to the Internet: the EU has long been a champion of freedom of expression and the free flow of information online. Allowing private actors to arbitrarily restrict certain uses of the Internet in the EU would validate the repressive practices of certain governments and other entities abroad that regularly stifle freedom of expression and the free flow of information.

As a matter of fact, European operators' restrictive behaviour is already sending the wrong signal abroad in relation to barriers to trade and freedom of expression, information and communication. Indeed in at least one major country outside the EU, we have already witnessed the examples of European and American companies' discriminatory practices towards Skype being used to justify that the government ban access to Skype and to the services of other foreign providers<sup>19</sup>.

These risks have already been recognized by the guardian of the European Convention of Human Rights, the Council of Europe, which decided to develop a Ministerial Declaration on Network Neutrality and Freedom of Expression.<sup>20</sup> The European Commission is duty-bound to similarly address the issue, and the proposals made above, notably the adoption and protection of a very clear open Internet principle across the EU in furtherance of the principles contained in the revised Electronic Communications Framework, address these concerns and would enable the EU to continue to lead by example in championing fundamental freedoms at home and abroad.

Should you require any additional information with regard to the contents of this response, please do not hesitate to contact us.

Yours faithfully,

Jean-Jacques Sahel | Skype


Director, Government and Regulatory Affairs | Europe, Middle-East & Africa  
SkypeID: jsahel  
e-mail: [jean-jacques.sahel@skype.net](mailto:jean-jacques.sahel@skype.net)

---

*Pepperdine Law Review, Vol. 36, 2008, [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1335055](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1335055).*

<sup>19</sup> Skype will liaise with the Commission separately on this point.

<sup>20</sup> <http://www.coe.int/t/dghl/standardsetting/media/>



## **ANNEX 1: Traffic management techniques that can be deployed in the mobile environment to block or degrade certain traffic**

Mobile operators use 3 main techniques to filter Internet traffic. It is important to note that the technical tools available nowadays enable operators to filter traffic even when it is travelling in their network at high speeds (gigabits/s) and with a precision that allows them to pinpoint and discriminate against specific applications, software or types of content<sup>[2]</sup>:

- i. **Through GGSN (Gateway GPRS Support Nodes) HTTP Proxies [network nodes]**, which can block access to individual http webpages or entire domains (e.g. www.skype.com). These systems are normally used to block illegal sites such as those with illegal adult content as identified by entities such as the Internet Watch Foundation in the UK. However the same systems can be utilised to block any site based on operator configuration. Access to a domain (e.g. skype.com), or the download pages on that domain, can be restricted specifically by including the relevant pages in the filter list. Until last year for example, several mobile operators around the EU used this method to bar access to the Skype.com website, some of them placing it without any justification whatsoever under their parental control filter, and it took almost two years of bilateral discussions for this filter to be removed.
- ii. **Through firewalls or other edge nodes**, These are usually designed to prevent unsolicited inbound connections to prevent attacks on the operator's network or mobile devices with viruses, trojans or exploitation of operating system security vulnerabilities to gain control over the target. Importantly these same nodes can also block users' outbound traffic so if for instance a certain user wanted to access a certain Internet protocol (IP) address range, or use certain ports, the mobile operator could decide for each individual user or for each subscription type, protocol, port or type of application that should be blocked or charged at a higher rate. The ranges or ports used by a particular software can be specifically targeted.
- iii. **Through special routers or other edge nodes** with techniques such as 'Deep Packet Inspection' or heuristics that allow the operator to analyse in real-time intelligence on the traffic coming from a user then decide whether to block or degrade it. This method can again be used at individual user level or through categories (such as per particular age or subscription profile) or at network-wide level. Voice and video packets of specific VoIP applications can be specifically targeted for example.

The technical filtering and blocking policies are implemented by configuration files that are deployed on the nodes (equipment) that are used to control the traffic. Such configuration files typically have to be recorded by operators for operational reasons (such as for troubleshooting or to upgrade systems procedures) through dedicated log trails which could potentially be analysed to determine past policies and 'box' configurations. Such logs are usually stored for months, typically a year.

The OECD reproduced in its '*Internet Traffic Prioritisation*' report (*OECD: INTERNET TRAFFIC PRIORITISATION: AN OVERVIEW (DSTI/ICCP/TISP(2006)4/FINAL, www.oecd.org/dataoecd/43/63/38405781.pdf*) ) the marketing material from a vendor of blocking technologies, copied below, which illustrates well with how much precision operators can affect the traffic of certain applications, services or content, with clear potential for subtle / covert

harmful behaviour: it ranges from a particular type of online game such as the popular *World of Warcraft* to messaging and VoIP applications such as Apple's *iChat* and Skype. This information dates back to 2006, and the technology has both improved and become cheaper to acquire.

**Table 1. Sample of applications that can be monitored, controlled and prioritised**

Peer-to-Peer	Voice over IP	Multimedia	Gaming	Messaging
Aimster	CiscoCTI	Abacast	Asheron's Call	AOL (IM,
Apple-iTunes	Clarent	Motion Video using	Battle.net	Talk, Image,
AudioGalaxy	CUSEeMe	DIGStream	Diablo II	File, ISP)
Bit Torrent	Dialpad	MPEG (Audio, Video)	Doom	iChat
Blubster	H.323	Multi-cast NetShow	EverQuest	ICQ
DirectConnect	I-Phone	NetMeeting	Half-Life	IRC
EarthStation V	iChat	Ogg over HTTP	Kali	Lotus IM
EDonkey	MCK Commun.	QuickTime	LucasArts (Jedi)	MSN
Emule	Megaco	RadioNetscape	MSN Zone	Messenger
Gnutella	Micom VIP	Real (Audio, Video)	Mythic	Windows-
Grokster	MGCP	RTP	Quake I, II, & III	POPUP
Groove	Net2Phone	RTSP	SonyOnline	Yahoo!
Hopster	RTP	SHOUTcast	Tribes I, II	Messenger
Hotline	RTCP	Streamworks	Unreal	
iMesh	SIP	VideoFrame	Warcraft III	
Limewire	Skinny (SCCP)	WebEx	WorldofWarcraft	
KaZaA	Skype	WinampStream	XboxLive	
KaZaA Lite	T.120	WinMedia	Yahoo! Games	
Morpheus	VDOPhone			
Napster	Vonage			
Napigator				
<b>+ 50 others</b>				

Source: Packeteer at <http://www.packeteer.com/resources/prod-sol/ApplicationDiscovery.pdf>