BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

EUROPEAN DIGITAL RIGHTS

Response of
Bits of Freedom and EDRi
to
the public consultation of the European Commission
on the open internet and net neutrality in Europe

30 September 2010

1. The Dutch digital rights organisation Bits of Freedom ("**Bits of Freedom**") and the European digital rights organisation European Digital Rights ("**EDRi**") would like to take this opportunity to respond to the public consultation of the European Commission on the open internet and net neutrality in Europe.

2. In short, Bits of Freedom and EDRi conclude as follows:

   - An open internet is crucial for fundamental freedoms, innovation, and competition.
   - Internet providers, however, have incentives of their own to stifle the open internet.
   - Furthermore, governments and private parties attempt to force internet providers to stifle the open internet for the benefit of narrow sectoral interests.
   - And in practice, internet providers do indeed stifle the open internet for the above reasons.
   - Meanwhile, transparency obligations, competition and minimum guarantees cannot safeguard an open internet.
   - Waiting is not an option, as the examples of local loop unbundling and mobile roaming demonstrate.
   - Narrowly-tailored regulatory EU measures should therefore safeguard the open internet.

An open internet is crucial for innovation, fundamental freedoms, and competition

3. Fast broadband truly is the "oxygen of the modern age", as Commissioner Kroes recently pointed out.[1] And similarly, the internet may rightfully be called modern humanity's lungs. In a similar manner as the bronchial tubes transport oxygen into the blood stream through many interconnections and branches, the internet transports information, ideas and services between people all over the world through a web of interconnected networks.

4. It is the duty of the governments of our information society to keep this vital infrastructure healthy, accessible and open. The importance of the internet has, for example, already been recognized by the government of Finland by enshrining in law a right to access the internet.[2] Likewise, the French Constitutional Court ruled in the HADOPI-case that internet access forms part of the fundamental human right to freedom of expression.[3] And it has widely been reported that Chile is one of the first countries to even protect net neutrality in its law.[4]

5. As correctly pointed out by the European Commission in its questionnaire, the end-to-end principle is one of the central design principles of the internet. In a network designed according to this principle, the network's users (or nodes) have a maximum freedom to communicate with each other and to innovate. Abandoning this principle, handing over control over communications at the core of the network, would essentially transform these user freedoms into provider powers. This power would be imposed as a result of capricious business priorities, with the help of changing control technologies and at the whim of government and/or media pressure.[5] Given the public interests which are at stake, this should not be allowed: internet providers must be obliged to respect these user freedoms.

6. It is widely recognized that the end-to-end principle has proved to be central to innovation, fundamental freedoms and competition:

    - **Innovation** The question of innovation is essentially a simple numbers game: the more people that are in a position to innovate, the more innovation will take place. The end-to-end principle results in a network which harbours as little assumptions as possible about the services it carries. With an open internet that respects the end-to-end principle, all users and application developers have the possibility to access and offer their innovative services and applications over the internet. This has allowed garage-inventors to become globally operating multibillion dollar companies, such as Google and Skype, without having to ask permission from internet service providers (“**ISPs**”) before they started offering their services to their customers. A network which - on the other hand - places a significant amount of application-specific functionality in the network's core, places primarily the network owners and internet access providers in a position to innovate, instead of its many users. The kinds of strategies and incentives that a non-neutral network creates is neatly shown not just by the fact that VoIP services have been blocked in the mobile environment, but also by the sheer range of blocking tactics used.[6] A modern information society can simply not afford this.

1 See http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=6070.
2 See http://www.bbc.co.uk/news/10461048.
3 See http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009-580DC-2009_580dc.pdf.
4 See http://translate.google.com/translate?js=y&prev=_t&hl=en&ie=UTF-8&layout=1&eotf=1&u=http://www.camara.cl/prensa/noticias_detalle.aspx%3Fprmid%3D38191&sl=es&tl=en.
5 See http://blog.indexoncensorship.org/2010/09/08/censorship-craigslist/.
6 See http://news.bbc.co.uk/2/hi/business/6901945.stm.

- **Fundamental freedoms** The open internet enables all users to connect to any other user that wishes to accept such connection. Thus, in the open internet, users can all freely communicate, fully express themselves, access information and participate in the public debate, without unneccessary interference by gatekeepers or middlemen. The end-to-end principle provides an important safeguard against censorship, both by public and private actors. The end-to-end principle does not imply that interference with users' traffic is not allowed at all, but ensures that such interference within the network is only allowed to the extent that this is strictly necessary and in the interest of the users. For example, under the end-to-end principle, filtering of content which some users do not desire to receive (such as spam) should not occur within the network itself, unless it is impossible to correctly implement this function at the edges. Since content which may not be desired by an individual user can also be filtered at the edge, the network provider should not be allowed to implement this function. Similarly, although at first sight it may be attractive for governments to use the possibility of greater control over the network as means of enforcing regulations, this also violates the end-to-end principle and leads to censorship. For example, governments should take measures against the distribution of images of sexual child abuse, not by blocking access to such websites (while keeping the images online), but instead by taking the images down and taking real and effective action against the perpetrators of these crimes.
- **Competition** As a result of the open internet, all applications can be offered over the internet, without interference by ISPs, and this leads to a flourishing of competition of services offered over the internet. For example, VoIP-telephony can in an open internet compete with non-IP telephony, thus bringing prices down and increasing quality of telephony services. In addition, abandoning the end-to-end principle for the internet and placing more functionality at the network's core than strictly necessary, negatively affects the application and content markets which are being offered over the top of the internet with any imperfections in the market of the network and internet providers.

Internet providers have incentives of their own to stifle the open internet

7. The end-to-end principle was until some years ago, generally respected. ISPs generally merely transported data between the users at the ends of the network on a best effort, first-come-first-served basis. ISPs did not pick favourites among applications or content, affording maximum freedom to the users of the network.

8. This, however, is changing quickly. Internet providers have the means, the motive and the opportunity to exercise further-reaching control over the internet traffic they transport:

    - **Means** The technology to make a distinction between various types of traffic is becoming increasingly sophisticated, thus giving ISPs the means to throttle and block internet traffic, often in ways which are very difficult to detect.
    - **Motive** In addition, ISPs are increasingly (vertically) integrated, also offering television, telephony and internet (content) services. ISPs consequently have a motive to block or degrade internet traffic which directly competes with the services they are offering. In addition, ISPs have an incentive to block indirect competition, for example by charging money from one service provider, promising to degrade the traffic of a downstream competitor.
    - **Opportunity** Lastly, ISPs currently are legally allowed to take measures blocking,

degrading or throttling traffic. It is not likely that end-users can succesfully lodge a claim against such practices, especially since such measures have not been prohibited in the recently amended Universal Service Directive.

9. We contest that the “rapid developments in the volumes of traffic passing over the internet” – as pointed out by the Commission in its questionnaire – would be responsible for the fact that net neutrality has recently become a hot topic. Scarcity in bandwidth has always been present in the telecommunications industry; only recently have ISPs seriously started to consider and explore business models which give them more control over traffic flows and applications in order to better exploit this scarcity and only recently have technologies become available (at a price) that make such practices feasible. If the supply of bandwidth in the past years has lagged behind the growing demand, this should in fact be ascribed to the lack of investments by ISPs in bandwidth and use of high overbooking factors. From the 2000 Communications review through the LLU Regulation and the most recent Communications review, the access industry argued against regulation on the basis that it would be detrimental to investment - which has consistently proven not to be the case.

Governments and private parties attempt to force internet providers to stifle the open internet

10. Not only do internet providers at their own initiative try to seize more control over internet traffic but internet providers are also increasingly under pressure from third parties to take measures which run counter to their role as a mere conduit:

- Firstly, **copyright holders increasingly pressure internet providers** to block traffic which is alleged to be infringing on their rights. Often, this is done through private negotiations - despite the fact the widespread restrictions on communication must have a legal base, in order to be compliant with the ECHR. As a first example thereof, UK internet provider Virgin Media concluded an agreement with UK collecting rights association, promising as an experiment to inspect the traffic of all its customers on infringing content.[7] The latest leaked draft of ACTA also pushes for such private negotations (see art. 2.8, *"Each Party shall endeavor to promote cooperative efforts within the business community to effectively address (US: copyright and related rights) (EU/J: intellectual property rights) infringement while preserving legitimate competition and consistent with each Party’s law, preserving principles relating to freedom of expression, fair process, and privacy, (EU: among other (US: fundamental) principles).”*). In addition, it has been extensively discussed to inspect and filter internet traffic on infringing content within the European Commission's Stakeholders' dialogue on illegal up- and downloading, as follows from recently leaked documents.[8]
- Secondly, **governments increasingly pressure internet providers** to filter or block traffic which is alleged to be illegal. Currently, many countries in the European Union are considering or implementing obligations on providers to block websites containing images of sexual child abuse, gambling websites and websites hosting other material.[9]

7 See http://www.theregister.co.uk/2009/11/26/virgin_media_detica/.

8 See http://www.pcinpact.com/actu/news/59106-hadopi-dpi-vedicis-scpp-filtrage.htm and http://www.pcinpact.com/actu/news/59102-hadopi-bruxelles-filtrage-blocage-europe.htm.

9 See the recent editorial in the EDRi-gram:: Belgium (gambling), Bulgaria (gambling), France (gambling and intellectual property), Italy (gambling, intellectual property, free online advertising, defamation, cigarette import, steroid advice) and Lithuania (gambling), to be found at http://www.edri.org/edrigram/number8.18/10-weeks-until-internet-blocking).

11. These developments may appear at first sight to be different from the "classic" issues of net neutrality, as internet providers do not take these measures at their own initiative or for their own benefit but do so under pressure from a third party. Upon further inspection, however, these developments are very relevant for net neutrality, since these affect the status of the internet provider as a mere conduit. There is a strong public interest in protecting this status, just as there is a strong public interest in protecting the status of the transporter of letters as a mere conduit. The fact that internet providers take measures at their own initiative to control the internet traffic of their end-users, influences the possibility to resist any measures imposed on them by third parties and vice versa.

And internet providers in practice do stifle the open internet

12. There are already various examples of highly controversial and downright abusive measures of ISPs taken in- and outside the European Union, stifling the open internet, which clearly demonstrate the urgent need for regulatory intervention to protect the open internet. Here are some examples, which do not pretend to give a complete overview of infringements in the European Union and outside:

- **2005: American ISP Madison River blocks VoIP** Madison River Communication, a small US ISP blocks the traffic of internet telephony application Vonage.[10] It is evident that the blocking is intended to favor its own VoIP-services, stifling competition. After this comes to light, the Federal Communications Commission intervenes.
- **2005: Canadian ISP Telus blocks access to union website** In 2005, the Canadian internet provider Telus during a strike of its union workers, decides to block access for all its customers to the union website, thereby stifling public debate.[11]
- **2008: Dutch ISP KPN wants to charge for streams of public broadcaster** In 2008, Dutch ISP KPN states that it cannot properly deliver the streams of the Tour de France and the European Football cup provided by the public broadcaster.[12] While other ISPs appear not to have a problem, KPN asks a remuneration from the public broadcaster for the transmission of the data. The provider and the public broadcaster do not come to an agreement, and ultimately only 10.000 customers of KPN can simultaneously watch the online transmissions of the public broadcaster.
- **2008: American ISP Comcast throttles peer-to-peer traffic of customers** US ISP Comcast in 2008 admits that it throttles peer-to-peer traffic of its customers.[13] The FCC prohibits this because it restricts competition. Comcast appeals the decision of the FCC, and the Comcast-case again sparks the discussion about net neutrality in the United States.
- **2008: Bell Canada starts throttling traffic of their residential wholesalers** before it hits their networks without telling those ISPs they were doing so.[14]
- **2009: UPC throttles peer-to-peer traffic of customers** In 2009, it turns out that Dutch ISP UPC also throttles peer-to-peer traffic.[15] The Dutch consumer association (the *Consumentenbond*) lodges a complaint with UPC and Dutch telecom regulator OPTA also intervenes. UPC and the Consumentenbond settle, UPC promises to stop its

10 See http://www.bloomsburyacademic.com/pdf%20files/NetNeutrality.pdf (p. 35).
11 See http://boingboing.net/2005/07/24/phone-company-blocks.html.
12 See https://zoek.officielebekendmakingen.nl/blg-35874.html.
13 See http://news.cnet.com/8301-10784_3-9878841-7.html.
14 See http://www.dslreports.com/shownews/Bell-Canada-Confirms-Throttling-92973.
15 See http://www.consumentenbond.nl/actueel/nieuws/nieuwsoverzicht_2009/UPC_moet_afknijpen_melden.

throttling practices and prevents an injunction.

- **2009: Dutch mobile service providers block Skype on mobile** In 2009, it follows from an investigation from the Ministry of Economic Affairs that various mobile internet service providers block competitor Skype. Under pressure from public opinion, some providers suspend the blocking of Skype, although we received a report (not confirmed) that KPN still blocks Skype on mobile.[16]
- **2009: UK ISP PlusNet blocks streaming application Spotify**, by applying a prioritisation scheme, slowing traffic classified as peer-to-peer traffic to 50 kbps on lines advertised as up-to 20 mbps. Spotify, a streaming media service, is listed as a peer-to-peer service in 2009, greatly slowing the speed of this and making it unusable.[17]
- **2009: Spanish incumbent Telefonica announces throttling services** In 2009, was been reported in the press that Spanish incumbent Telefonica will offer subscriptions with differing service levels, implying that in the case of congestion subscribers who pay more will be prioritised.[18]
- **2009: United States internet provider RCN settles lawsuit for blocking p2p-traffic** In 2009, internet provider illegally started interfering with peer-to-peer-traffic.[19] After a class action was filed, RCN settled, promising to stop throttling peer-to-peer traffic for 18 months.
- **2009: Mobile internet provider Vodafone puts in place p2p and VoIP caps** on internet traffic in Italia, by capping this traffic on 64 kbit/s on its mobile network from 7 AM to 10PM.[20]
- **2010: Deutsche Telekom wants to be paid for traffic from Google and Apple** Deutsche Telekom in July 2010 announces that it wants to develop new payment models for mobile internet.[21] It wants to inter alia demand that service providers, such as Google and Apple, pay for tranmission. It is to be expected that many providers of internet access will abuse their bottleneck position in this manner to generate more revenue.
- **2010: Deutsche Telekom announces that it will block Skype** In 2010, T-Mobile announced that it will block Skype traffic on smartphones with a mobile internet connection, and is even considering blocking Skype through its wifi hotspots.[22]
- **2010: Swedish mobile telephony provider Telia blocks VoIP and p2p-traffic**, according to the advertisements on their website.[23]
- **2010: French provider SFR sells iPad subscriptions without access to p2p, VoIP and newsgroups**, although it is not clear whether these are contractual or also technical restrictions.[24]
- **2010: French internet provider "Free" restrict p2p, ssh and VoIP services on ADSL** According to Free, all ports and/or protocols which are not standard are blocked in the afternoon, such as SSH, streaming videos, VoIP and p2p.[25] The company's online

16 See https://zoek.officielebekendmakingen.nl/blg-35874.html.

17 See http://community.plus.net/forum/index.php/topic,75288.0.html.

18 See http://advocacy.globalvoicesonline.org/2010/09/13/telefonica-spain-and-net-neutrality/.

19 See http://broabandtrafficmanagement.blogspot.com/2010/04/rcn-sorry-we-will-stop-doing-that-p2p.html.

20 See http://www.areaaziende.vodafone.it/190/trilogy/jsp/programView.do?tk=9610,c&channelId=-8671&contentKey=48195&programId=12545&ty_key=az_uso_equo_servizio_internet_mobilita&pageTypeId=9610&ty_skip_md=true.

21 See: http://tweakers.net/nieuws/68724/t-mobile-wil-dat-google-gaat-betalen-voor-gebruik-mobiel-netwerk.html.

22 See http://www.handelsblatt.com/technologie/mobile-welt/telekom-plant-skype-blockade-fuer-iphone-und-blackberry;2219922.

23 See http://www.telia.se/privat/produkter_tjanster/mobilt/surfaimobilen/.

24 See: http://www.iptegrity.com/index.php?option=com_content&task=view&id=548&Itemid=9.

25 See http://www.numerama.com/magazine/15461-free-briderait-les-protocoles-ssh-voip-ou-p2p-en-zone-non-degroupee.html see http://pastebin.com/MZ3WF8sz.

helpdesk states that only p2p is blocked.

- **2010: Internet provider Telenor in Sweden does not allow IP-Telephony** on some mobile broadband options.[26]
- **2010: Incumbent internet provider Telecom Italia caps p2p-traffic in over 40 cities**. This is under investigation by the Italian telecommunications authority.[27]
- **2010: BT and TalkTalk would give priority to a specific streaming video** service depending on who pays. PCPro reports on 28 September that the UK's two biggest ISPs have openly admitted they'd give priority to certain internet apps or services if companies paid them to do so.[28]

13. When we refer to breaches of net neutrality, we do not just refer to traffic discrimination but also the manipulation of integral parts of the network. One such example is the ISP's DNS-server, which operate over the network, but are sometimes used to implement blocking of blacklisted websites.[29] One can also think, for example, of email servers of ISPs, which are also servers operating over the network, but are generally expected to deliver to the recipient all email they receive. This, however, is not always the case.[30]

14. In addition, network neutrality also is closely related to technology neutrality. One should be able to use all devices and applications for use over all types of infrastructure, even if this has been restricted by technological or contractual measures.

Transparency, competition and minimum guarantees only cannot safeguard an open internet

15. Firstly, it should be noted that most ISPs have an incentive to limit bandwidth and discriminate between various types of traffic. Each provider has the same incentive to maximise its revenue, and one way to do it is by discriminating between different types of traffic. Consquently each provider has an incentive to discriminate traffic over its internet lines. It is also relevant that already a large part of ISPs in the European Union are vertically integrated. These vertically integrated ISPs even have additional commercial incentives to block traffic from direct or indirect competitors. This also leads to uncertainty at the end of service providers, who cannot reliably estimate the user base available to them - since they may be cut off from their user base by a provider which deems it fitting to degrade the traffic of potential competitors. This, consequently removes the incentives for investing in innovative services.

16. Thus, it is to be expected that, even if it is assumed that the transaction costs of switching from one provider to another are negligible, still the openness of the net will be diminished if

26 See http://www.telenor.se/privat/abonnemang/tillaggstjanster/alla-mobiltjanster.html#C45-2100-P45-5468.

27 See http://www.aiip.it/page.php?id=952&aiip=4f21c777739f159beb86d9d49d9e9200 and http://www.187.alice.it/cda187/c/assistenza/newsPopupAction.do?ID=19784 and http://nbtimes.it/attualita/eventi/5988/neutralita-di-rete-e-servizi-agcom-chiede-chiarimenti-a-telecom-italia.html.

28 See http://www.pcpro.co.uk/news/broadband/361501/talktalk-bt-wed-put-iplayer-in-the-slow-lane.

29 See the EDRI-gram: http://www.edri.org/edrigram/number8.18/10-weeks-until-internet-blocking.

30 American ISPs SBC Global and Earthlink censor e-mail Notwithstanding the fact that SBC and Earthlink subscribers had expressly chosen to receive e-mail and news updates from conservative news sites such as NewsWithViews, these ISPs blocked emails from this source, and SBC Global apparently also blocked emails from at least four other conservative newsletters, see http://www.newswithviews.com/NWVexclusive/exclusive114.htm. In 2005 American ISP Comcast censors e-mail Comcast filtered any e-mails from anti-war organization AfterDowningStreet (now known as War Is A Crime .org), without those clients having asked Comcast to do so or even being told that Comcast did not allow any incoming mails from AfterDowningStreet to reach their inboxes. In addition, Comcast never notified the organization it was blocking e-mails from. This practice caused a severe restriction on the freedom of AfterDowningStreet to participate in the public debate and on Comcast's clients to receive information, see http://warisacrime.org/node/794.

only transparency obligations are imposed.[31]

17. The assumption that transaction costs would negligible, however, is false. There are various reasons why in fact switching from one provider to another is quite difficult, if not downright insurmountable:

- Most vertically integrated ISPs in the European Union currently offer triple-play packages – i.e. with internet access, telephony and television – to their customers. If one were to switch to another provider for internet access, a customer would lose the reduced price of the triple play-package. This poses a serious switching barrier.
- Internet access is for many European citizens already an essential service. When switching internet provider, this may lead to a lack of connectivity for a period of time, in some cases two days and in others several weeks. The risk of being cut off from internet connection for more than a day is for many people a reason for not switching in the first place.
- This ties into the fact that a EU customers have had bad experiences when switching from one operator to another in other markets. It follows from research from Heliview for the Dutch Ministry of Economic Affairs from 2005 that almost 1 out of 3 consumers indicates that because of a bad experience when switching in the fixed telephony market, they will not switch again.[32]
- In some countries, a customer is offered an email address together with an internet acess subscription. Email-addresses are not portable, and consequently, switching to a different internet access provider means losing your email address. This is an important switching barrier for almost all customers.

18. It follows from the above, that transparency obligations alone cannot safeguard an open internet.

19. In addition, it should be noted that the application of competition law cannot safeguard an open internet. End-users will have a difficult time arguing that measures restricting network traffic are contrary to competition law. It will often be difficult to prove, for example, that throttling at the initiative of the provider would significantly restrict competition, and it will be even more difficult to show that this can be considered abusive, especially since these practices are arguably currently implicitly allowed under the Universal Directive.

20. Lastly, the minimum quality of service requirement as set out in the Universal Service Directive cannot guarantee the open internet. If this requirement is to be interpreted in such a way as to state that a non-discrimination obligation (as set out further below) should only apply to a certain minimum amount of bandwidth, it would be a good start but it would leave the other part of the bandwidth open for discrimination. Given the fact that high-bandwidth applications are partly the kind of services which will be subject to throttling, blocking or degradation, such a solution would only partly solve the problems set out in this contribution. In addition, these measures would only be applied by national regulatory authorities, and not

31 See also Benkler, p. 158 and 159: "*Under anything less than a hypothetical and practically unattainable perfect market in communications infrastructure services, users of a proprietary infrastructure will face a less-than-perfect menu of influence exactions that they must accept before they can communicate using owned infrastructure*." To be found in: http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf,

32 See the presentation "Beleidsworkshop Consumenten en Mededinging", 15 december '05# Introduced by Martin bij de Leij, available at: http://www.encore.nl/documents/pres_BijdeLeij_extern_000.ppt.

have a Europe-wide effect.

Waiting is not an option, as local loop unbundling and mobile roaming demonstrates

21. It appears at first sight attractive to refrain from regulation, and only intervene if the problems pointed out are sufficiently severe. Waiting, however, is not an option. As set out above, the open internet is already under a severe threat and it is to be expected that ISPs will do everything in their power to delay regulatory intervention, thereby causing irreparable harm to the European economy and fundamental freedoms.

22. For example, in the recent past, we have seen mobile operators delay the adoption of binding legislation to prevent market abuses. Such delays have caused significant financial damage to European citizens and European businesses. A perfect example of this was mobile roaming, where citizens and businesses were paying unjustifiable costs for years. With a very motivated Commissioner determined to redress the balance, the process from the launch of the investigation by the European Commission until the approval of the Regulation 717/2007 being slightly more than two and a half years, during which time the abuse continued virtually unabated.

23. The history of local loop unbundling provides an even better case study. In March 2000, the Council approved local loop unbundling in principle, but the problems persisted. The next month, the Commission produced a Recommendation and then, in June, it produced a draft Regulation. Even in France, the country in Europe which was the most motivated to implement the Regulation as quickly and fully as possible, with an exceptionally impressive team in the NRA working full time on the dossier, it took until the end of March 2001 before a fully acceptable reference offer could be agreed with France Télécom. Effective implementation, took much longer in other countries and never happened in most of them - to the detriment of competition and, ultimately, consumers and business.

Narrowly-tailored regulatory EU measures should therefore safeguard the open internet

24. Given the importance of the open internet, and given the fact that transparently alone will not suffice, the European Commission should take effective and narrowly-tailored measures to safeguard the open internet. The goal stated in recital 28 of the Universal Service Directive 2009/136/EC should be the main focus of the policy of the European Commission:

> "End-users should be able to decide what content they want to send and receive, and which services, applications, hardware and software they want to use for such purposes, without prejudice to the need to preserve the integrity and security of networks and services."

25. This implies that ISPs should not be allowed to degrade or block services offered over the internet or slow down traffic or discriminate between different types of traffic over the internet (cf. recital 34 of the Universal Service Directive).

26. The only possible exceptions are where this would be necessary to (i) enable end-users to decide what content they want to send and receive, and which services, applications, hardware and software they want to use for such purposes or to (ii) preserve the integrity and security of networks and services. These exceptions to the main rule should be narrowly

tailored to meet a specific, necessary goal and be for the direct benefit of the end-user. This also requires that there are no less restrictive measures with the same or a similar effect.

27. Please note that we do not argue that the internet is a 'finished product', which should remain exactly as it is. It is possible that innovations and intelligence within the network may be beneficial to internet users. We do argue, however, that the basic design principle that resulted in the internet becoming a vital fundament of our information society, should remain central internet policy. This main design principle, the end-to-end principle, has been described above.

28. Some short term problems, which deviations of the end-to-end principle are claimed to solve, such as better performance for specific applications like high definition IP-TV, can also be solved by means which do not damage the usability, flexibility and evolution of the network as a whole and which do not hand over user freedoms to the short-term commercial or public relations interests of access providers. If, for example, the backbone of an ISP is structurally filled with streaming video of a content provider, a proportionate measure to deal with such congestion would be to (i) upgrade the backbone, and/or (ii) install content delivery servers at the end of the network, which replicate the stream from the backbone (edge caching). By having content providers colocate servers at ISPs' facilities close to the end users, one can reduce the need for transit agreements, and considerably unburden the internet backbone. This example also demonstrates that the options presented by the Commission in the face of congestion are not complete ("*where a network starts to experience regular and disruptive congestion […] the network operator is faced with two general options: – increase the capacity of the network to meet demand; – differentiate between traffic on the basis of origin, destination or content type*").

29. This principle should apply to fixed and mobile networks in the same way. The only relevant distinction between these two could in theory be the fact that there allegedly is more scarcity in mobile networks. If this were true, it would, however, mean that providers should further invest in mobile networks in order to deal with such scarcity. The fact that mobile operators have invested billions of dollars in UMTS-licences should provide an indication for the fact that they indeed expected an enormous growth in demand. It is their responsibility now to meet this demand. And as it will become increasingly common to connect to the internet via mobile networks, it will become increasingly important to enforce the same rules over moble networks. Furthermore, distinct rules for distinct networks would stop convergence in its tracks.

30. In the discussion about net neutrality, a distinction is sometimes made between "managed services" and the best-effort internet. If these "managed services" were to be offered via public IP-address, they would in fact form part of the internet, and the rule set out above should apply. Exclusive arrangements between network operators and content providers to provide such managed services that would have impact on the communication freedom of the end user, shall under the rule set out above generally not be allowed. To agree on such exclusivity is not "necessary" to provide such content – YouTube, iTunes and other content providers are already currently able to serve their content without exclusivity, and ISPs are able to deliver the service to the end-user already. Any costs related to upgrading the network will have to be borne by individual subscribers, not by charging various content providers for not degrading their traffic (the so-called "Tony Soprano" model of networking).

If these managed services are provided over infrastructure which also carries public IP-traffic, but is not itself part of the public internet, transparency is required about the bandwidth allotted to the public internet offered to a subscriber – and the fact that this bandwidth may be restricted if managed services are used over the same carrier. Furthermore, there is a risk that investments in managed services would undermine the investments in the internet.

31. Such a rule should be in the form of regulation, not by industry code of conducts. ISPs have – as set out above – an incentive to throttle, degrade or block traffic. Any code of conduct agreed on between ISPs will reflect this incentive, even if consumer assocations have been consulted. The open internet is a matter of public interest and the protection thereof should not be in the hands of those who have a powerful incentive to stifle the open internet. These rules should be made on a European Union level, in order to ensure an open internet across the European Union.

32. As regards transparency, full transparency should be imposed. Bits of Freedom has set out transparency requirements to the Dutch Ministry of Economic Affairs. For the sake of brevity, we refer to the requirements of full transparency set out therein (see annex, in Dutch).

33. EDRi remains available to further explain the above at your earliest convenience. You can contact EDRi through:

Joe McNamee - Advocacy Coordinator
Tel: +32 2 550 4112
E-Mail: joe.mcnamee@edri.org

* * *