

Hello,

here are my personal answers to your consultation to net neutrality.

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?

There are several problems.

1) According to the HADOPI-law in France people could be denied internet access if there have been multiple copyright infringements via their internet connection.

The internet has evolved that fast, that for normal citizens it is nearly impossible to uphold their personal security. Through malware it is possible to redirect traffic through the computer of other people. Normal users are unable to protect their computers properly. Using wireless networks people could access the internet via the internet connections of someone else. There are known vulnerabilities in wireless protection algorithms like WEP or WPA.

People rely more and more on the internet. Most companies require a person to have an email-address for a job application. A lot of expert knowledge is only served on the internet. To deny someone internet access, means to deny him a chance for a new job or further training.

2) Some countries like Sweden or Denmark manipulate DNS entries to deny access to illegal content like child pornography. While this method is not effective and does not remove the content or sue the producers and distributors, it affects the reliability of one of the core services of the internet (DNS). The internet is based on standards. Many automated processes rely on correct answers according to the protocol specifications. To falsify the reply of a domain handling many legit offers could have a massive impact. For example many black and white listing services for spam rely on DNS answers. An incorrect response to a white-list or black-list could deny or allow the server to send emails. The methods used to manipulate the requests are the same methods used by hackers to gain access to company networks or to redirect users to a malware site. It is not possible to close the security holes for hackers while keeping them open for blocking illegal websites.

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

Many countries try to apply local law to the internet. Most people who try to do so, have problems to understand the nature of the internet. While there is a need for regulatory controls they could not be handled by one country on its own.

- 1) To explain the problem I like to take an approach to protect minors in germany. There were the following ideas:
- adult content should only be aired during the night
  - every webpage should be categorized
  - not categorized pages should be blocked by the internet access providers

The internet is global and doesn't know conventional borders. I go shopping right around the corner on the United Kingdom, buy chocolate in Belgium or get some rare items from the United States. I buy some new wallpapers for my desktop from an artist in Japan. In the internet business is not bound to a local marketplaces. The idea of a special airtime for adult content is to be adapted from television. But there are a few problems, why this doesn't apply to the internet. A adult content provider in germany is airing adult content from 11:00 pm to 5:00 am, but the young customer just around the corner in Sydney is watching the content from 7:00 am to 3:00 pm. If you have access to pages from all over the world, there is always a timezone where it is airtime for adult content. But a german adult content provider would not participate in the business in other regions. The content providers don't know who and where their customers are. The access providers have only limited means to check the content of a transmission and are not supposed to use them.

Every webpage should be categorized and non-categorized content should be blocked by the internet access providers. If this would be local law, many foreign people won't know about it or won't comply with some strange german law. The effect would be that many foreign sites would not be available in germany. There would be a german internet and the rest of the world internet. This would be a massive set back.

There are also many different communication protocols on the internet. Many protocols that deliver content do not rely on conventional structures like a central server. For example a lot software and music (free and commercial) is distributed via so called peer2peer networks, to save bandwidth and minimize costs. In peer 2 peer Networks everyone could be consumer and/or distributor. This is a big chance for small companies and artist who wouldn't have the means to distribute their software or other content. A single artist could handle millions of customers all over the world. But on the other hand it allows bypassing the conventional distribution networks. Which endangers the business model of companies specialized in distribution. There are also people exchanging commercial content without paying royalties.

Instead of local approaches to regulate against standards, there should be global approaches to define new standards.

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

Yes and no. The framework is a nice base for controlling quality and power of conventional access providers.

The internet is beginning to change more and more there are alternate ways of access. Within mesh networks, every member is end user and access provider at the same time. For now most mesh networks are connected to conventional access providers. But over time the mesh networks will grow and there will be much

less "dedicated access providers". There are already citywide approaches for mesh networks. These technologies will provide much more redundancy and performance than conventional centralized networks. They will also counter the effects of local approaches to regulate and control the internet.

The regulatory framework is also not suitable for defining the role of non-commercial access providers (like owners of public hotspots).

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 always necessary. The easiest form of traffic management is packet scheduling and queue management. These technologies prevent single subscribers to block the whole bandwidth. Another option is quality of service. There are multiple legit applications for quality of service. The provider needs quality of service to ensure his own priority for maintenance and troubleshooting tasks. Many companies need a reliable bandwidth. To ensure the fulfillment of the service agreement the providers also use QoS. Another option would be to let the user prioritize his own traffic by tagging the packets. This is useful to ensure connections like VOIP or Multimedia will be favored. It is not one of the providers tasks to check and judge the traffic. A provider could not reliably distinguish an encrypted VOIP-connection from an encrypted download. A picture could not be easily distinguished from a steganographic message. The provider should not define priorities on assumptions about the content. Besides of lines with "ensured bandwidth" the bandwidth should be fairly weighted between end users. The users themselves should only be able to favor some connections over others. Otherwise users would masquerade traffic as a prioritized service to gain bandwidth.

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?

Transparency is important. In my opinion the distinction between managed services and services on a best-efforts basis will be very difficult. There should be a fair solution that fits for both.

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

Yes. The requirements are the same. Also there are no "guaranteed bandwidth" in mobile networks.

Question 7: What other forms of prioritisation are taking place? Do content and application

providers also try to prioritise their services? If so, how – and how does this prioritisation affect other players in the value chain?

---

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?

In general all service conditions should be offered to all normal customers. Also different service levels may have different costs. There might be special conditions for emergency services and disaster control.

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 prioritization of emergency-services and disaster control should be a regulatory one.

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?

In my opinion the peering agreements work. For content-providers it is difficult to estimate the traffic that is transmitted to their servers. Especially during distributed attacks the traffic could massively increase. For non-commercial hosters this could be existential high costs. There should be a solution, but I have no idea what.

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?

There need to be minimum service requirements to ensure emergency services. There should also be a reliable service level for the customer.

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

Minimum bandwidth and availability should be monitored and have to be ensured according to the service level agreed on.

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?

No idea.

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

It is important for customers to know what services they get and how they are supplied.

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?

Yes, there are several risks. There are several approaches (blocking of content or domains) that, are trying to produce the technical means for censorship. There are several approaches to enforce local laws which could split the internet in regional networks, with limited connectivity.

Other concerns:

Conventional roles are fading within the internet. These may lead to problems with laws that rely on those terms. For example there are only a limited number of news publishers that could reach nationwide audience. In the internet everyone could open a blog and reach an unlimited number of people, regardless of their geographical location. Within the internet everyone could distribute his goods worldwide. People with popular "non-commercial" sites, trying to get donation to cope with the expenses for hosting their site, could make as much money to be judged as commercial. Everyone could be distributor. This could especially lead to problems distinguishing between commercial use and hobby projects.

With kind regards

Tobias Morsches  
IT-Security Consultant  
Freiheit 8a  
D- 51429 Berg. Gladbach  
Germany