The EDRi papers
ISSUE 08

NET NEUTRALITY

EUROPEAN DIGITAL RIGHTS

Net Neutrality is the principle that every point on the network can connect to any other point on the network, without discrimination on the basis of origin, destination or type of data.

This principle is **the** central reason for the success of the Internet. Net Neutrality is crucial for innovation, competition and for the free flow of information. Most importantly, Net Neutrality gives the Internet its ability to generate new means of exercising civil rights such as the freedom of expression and the right to receive and impart information.

In this booklet, we will explain Net Neutrality, why it is important, why certain Internet access providers believe that they have an interest in violating it, and we will address common misconceptions.

“Allowing broadband carriers to control what people see and do online would fundamentally undermine the principles that have made the Internet such a success”.

- Vint Cerf, founding father of the Internet [01]

CONTENTS

Booklet written by:

Kirsten Fiedler, Advocacy Manager
Joe McNamee, Executive Director
With condtibutions by EDRi members

Edited by:
EDRi & Digital Courage (Germany)

Design by: CtrlSPATIE

European Digital Rights (EDRi) is an association of 35 privacy and digital civil rights associations from 21 Countries.

European Digital Rights
20 Rue Belliard
1040 Brussels
tel: + 32 (0) 2 274 25 70
brussels@edri.org

WHAT IS NET NEUTRALITY?

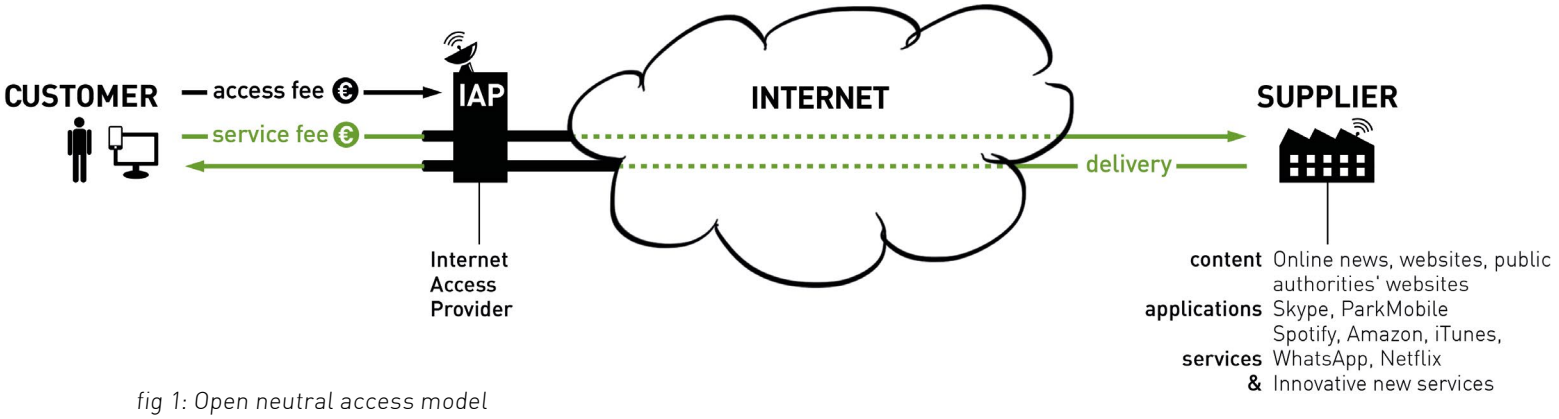

fig 1: Open neutral access model

FREEDOM OF COMMUNICATION IN THE DIGITAL ERA

The Internet is a global, interconnected and decentralised autonomous computer network. We can access the Internet via connections provided by Internet access providers. These access providers transmit the information that we send over the Internet in so-called data "packets". The way in which data is sent and received on the Internet can be compared to sending the pages of a book by post in lots of different envelopes.[02] The post office can send the pages by different routes and, when they are received, the envelopes can be removed and the pages put back together in the right order.

When we connect to the Internet, each one of us becomes an endpoint in this global network, with the freedom to connect to any other endpoint, whether this is another person's computer ("peer-to-peer"), a website, an e-mail system, a video stream or whatever.

The success of the Internet is based on two simple but crucial components of its architecture:

1. Every connected device can connect to every other connected device.

2. All services use the "Internet Protocol," which is sufficiently flexible and simple to carry all types of content (video, e-mail, messaging etc) unlike networks that are designed for just one purpose, such as the voice telephony system.

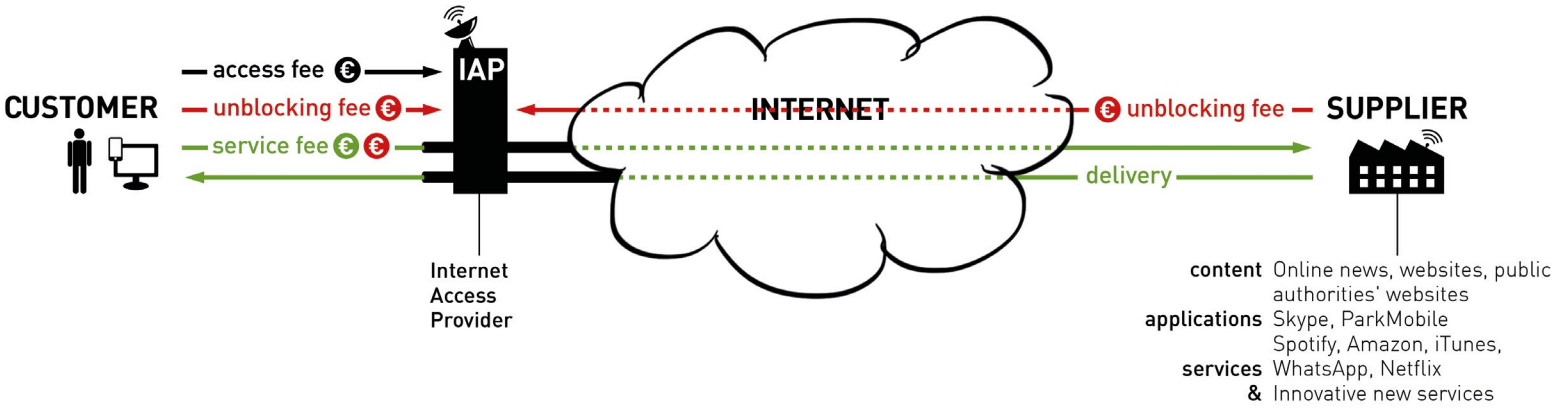

fig 2: Non-neutral access model

Net Neutrality is most commonly defined as the principle that Internet users can connect to any other point in the network. Users can create, access and use any content, service and application they choose, without discrimination, restriction or limitation imposed by those who run the infrastructure.

Internet access providers enable us to communicate, browse the web or transfer files over the Internet, to make our own websites globally available and to use services such as email, social media or Internet telephony. Everybody, and in whatever role, and all organisations, of whatever size and style, is able to participate globally. Everybody is able to access services and to offer services.

Let's say you want to watch a video online: You connect to the Internet, open your browser and navigate to the video service of your choice. This is possible because the access provider does not seek to restrict your options.

Without Net Neutrality you might instead find that your connection to video service A is being slowed down by your access provider in a way that makes it impossible for you to watch the video. At the same time, you would still be able to connect rapidly to video service B and maybe watch exactly the same content. Why would your access provider do such a thing? There are many reasons: for example, the internet access provider might a) have signed an exclusive agreement with this second video platform or b) provide their own video services and therefore want to encourage you to use these instead of the service that you initially preferred.

This is just one of the many reasons for violations of Net Neutrality. Such discriminatory measures are often called "traffic management". We will explain the most common reasons for violations of Net Neutrality in the following chapter.

"I don't believe that restricting consumers' choice can ever be an appealing driver of more growth. I certainly don't believe that restricting access to the internet will attract many more innovative European internet companies. And I don't believe that restricted access to the internet is the right answer to a faster deployment of Next Generation Access Networks."

- European Commission Vice President Viviane Reding, September 2008[03]

WHY IS NET NEUTRALITY VIOLATED?

THE THREE MAIN REASONS

There are many reasons why Net Neutrality is not respected, among the most frequent ones are:

Access providers violate Net Neutrality to optimise profits

Some Internet access providers demand the right to block or slow down Internet traffic for their own commercial benefit. Internet access providers are not only in control of Internet connections, they also increasingly start to provide content, services and applications. They are increasingly looking for the power to become the "gatekeepers" of the Internet. For example, the Dutch telecoms access provider KPN tried to make their customers use KPN's own text-messaging service instead of web-based chat services by blocking these free services. Another notable example of discrimination is T-Mobile's blocking of Internet telephony services (Voice over IP, or VoIP in short), provided for example by Skype, in order to give priority to their own and their business partners' services.

Access providers violate Net Neutrality for privatised censorship

In the UK, blocking measures by access providers have frequently been misused to block unwanted content. For instance, on 4 May 2012, the website of anti-violence advocates "Conciliation Resources" was accidentally blocked by child protection filters on UK mobile networks[04]. Another example is Virgin Media. The company provides access to the Internet and increasingly uses Deep Packet Inspection (DPI – see box on page 9). Virgin is now using this same privacy invasive technology to police their network in attempt to protect its own music business.[05] In all of these cases, private companies police their users' connections to censor what they guess may be unwanted content.

Access providers violate Net Neutrality to comply with the law

Governments are increasingly asking access and service providers to restrict certain types of traffic, to filter and monitor the Internet to enforce the law. A decade ago, there were only four countries

filtering and censoring the Internet worldwide – today, they are over forty.[06] In Europe, website blocking has been introduced for instance in Belgium, France, Italy, the UK and Ireland. This is done for reasons as varied as protecting national gambling monopolies and implementing demonstrably ineffective efforts to protect copyright.

Some politicians call for Net Neutrality and demand filtering or blocking for law enforcement purposes at the same time. However, it is a paradox to create legal incentives for operators to invest in monitoring and filtering or blocking technology, while at the same time demanding that they do not use this technology for their own business purposes.

Deep Packet Inspection (DPI)

Information that we send and receive through the Internet travels in so-called "packets", with "envelopes" indicating sender and receiver. Unlike normal network equipment, DPI looks not just at the envelopes but into packet contents, and can be used to disrupt or block certain packets based on what they contain.

DPI can be used for innocuous reasons (to fight spam or viruses), but also to carry out surveillance or to censor information as this technology makes it possible to capture information from network traffic and assess it in real time. In Russia for instance, Cisco's Deep Packet Inspection solutions are allegedly being used by the government to block access to certain websites.[07] Cisco's DPI tools are also being used in Germany by T-Mobile[08] on mobile networks.

10 reasons

for

NET NEUTRALITY

reason 01

No discrimination – Net Neutrality is the principle that all types of content and all senders and recipients of information are treated equally. This principle upholds the right to freedom of expression which includes, according to Article 19.2 of the United Nations' International Covenant on Civil and Political Rights (ICCPR), the freedom to seek, receive and impart information and ideas of all kinds. Without Net Neutrality, Internet access providers would become gatekeepers of the access to content on the Internet, with the power to decide what we can read and write and with whom we are allowed to communicate.

reason 02

Free Expression – The history of the Internet shows very clearly that Net Neutrality encourages creative expression. The ability to publish content and to express opinions online does not depend on financial or social status

and is not restricted to an elite. There is a huge trend towards people sharing information and experiences online, sometimes referred to as web 2.0. This means that individuals, small businesses, traditional news sources and large businesses can all create content that is available to everybody. Net Neutrality enables information to travel through the network without being restricted or blocked, thereby enabling a vibrant digital environment, full of ideas and innovation.

reason 03

Privacy – Measures to undermine Net Neutrality can have a direct impact on our privacy (DPI – see box on page 9). In a non-neutral Internet, providers would be able to monitor our communications in order to differentiate between messaging, streaming, peer-to-peer (P2P), e-mails and so on. According to a recent study, some European access providers are already doing so via the use of Deep Packet Inspection (DPI) for their commercial benefit.[09] The reuse of this technology for government or intelligence purposes is inevitable.

reason 04

Access to Information – Net Neutrality is also the catalyst for the creation of diverse and abundant online content. Non-profit projects like Wikipedia, blogs and user-generated content in general have the same conditions to access and publish information as large, commercial Internet players. Without Net Neutrality, we would have a two-tier Internet where only those who can pay would be able to access information or get content delivered faster than other users.

reason 05

Democratic Process – Net Neutrality improves the quality of democracy by ensuring that the Internet remains an open forum in which all voices are treated equally. It ensures that the ability to voice opinions and place content online does not depend on one's financial capacity or social status. It is therefore a powerful tool in facilitating democracy, enabling diverse ideas to be expressed and heard.

reason 06

Tool against censorship – Without Net Neutrality, network operators can block or throttle not only services,

"The concept of Net Neutrality builds on the view that information on the Internet should be transmitted impartially, without regard to content, destination or source. By looking into users' Internet communications, ISPs may breach the existing rules on the confidentiality of communications, which is a fundamental right that must be carefully preserved. A serious policy debate on Net Neutrality must make sure that users' confidentiality of communications is effectively protected."

- European Data Protection Supervisor (EDPS) on Net Neutrality,

but also content. The fundamental shift in information communications technologies over the last 10 years has facilitated revolutions and it offers the possibility of greater social reforms through greater transparency and the free flow of information.

reason 07

Consumer choice – Net Neutrality ensures access to content and offers greater consumer choice by allowing more players to enter the marketplace. Therefore, the amount of online information is vast and growing, leading to intellectual and cultural interaction that was scarcely imaginable twenty years ago. Without a neutral net, access providers can prioritise applications or services, thereby creating "walled gardens" in which consumer choice is limited.

reason 08

Innovation and competition – Net Neutrality continues to foster innovation, as individuals and companies alike can create content and provide new services with the online world as their audience. Any individual can upload content at relatively little cost. An unrestricted Internet gives market access to small and medium enterprises or start-ups that might not otherwise have a competitive edge against larger corporations. Without Net Neutrality however, access providers are allowed to restrict access needed by innovators that seek to develop online services. Innovators would have a smaller and less predictable marketplace for their services. For example, a start-up company might not be able to reach all access providers' customers, or pay potentially thousands of providers to do so.

reason 09

Digital Single Market – Net Neutrality is a cornerstone for the completion of the Digital Single Market. It removes barriers and allows users to freely communicate, fully express themselves, access information and participate in the public debate – without unnecessary interference by gatekeepers or middlemen. By contrast, a non-neutral Internet contributes to the fragmentation of the Digital Single Market. The European Parliament acknowledged this danger by adopting a resolution on "Completing the Digital Single Market"[10] in October 2012, in which it "calls on the Commission to propose legislation to ensure Net Neutrality".

reason 10

Protecting a global Internet – As soon as access providers start making use of traffic discrimination tools to interfere in global communications for their own commercial benefit, governments will be tempted to use the technology for public policy goals – in fact, Western governments are more and more often asking providers to restrict certain types of traffic, and to filter and monitor the Internet to enforce the law. In other parts of the world this has lead to "national Internets", such as the "Chinternet" in China and the "halal" Internet in Iran. The principle of Net Neutrality will help protect the global Internet.

Myths & Truths

Contribution by Access

Myth 1

Net Neutrality is bad for the development of infrastructure – who is going to pay?

The availability of content is a factor that stimulates broadband investment. Revenues from broadband and mobile access are dependent on demand for web-based content and applications. This has been empirically proven through the PLUM[11] study, which found that "the ability of consumers to access Internet content, applications and services is the reason consumers are willing to pay Internet access providers. Access providers are dependent on this demand to monetise their substantial investments."

Some Internet access providers argue that application and content providers "free-ride" on network investment made by others. This claim is baseless, because users already pay for content and applications, which allows access providers to profit from their investment in networks. Content and applications providers buy services from access providers, purchase network access and services. Moreover, consumers' demand to use high-bandwidth applications, such as peer-to-peer and streaming music and video, creates demand for faster Internet connections, more revenue for access providers and, ultimately, fuels investment in infrastructure.

Myth 2

Net Neutrality legislation would mean no network management, causing problems for the quality of the Internet

It is not true that legislation protecting Net Neutrality would prevent access providers from managing their networks. In fact, the Transmission Control Protocol ("flow rate fairness") that is at the core of Internet engineering has been one of the greatest congestion management tools that has helped make the Internet such a success.

What Net Neutrality would prevent is not traffic management, but rather arbitrary restrictions implemented by access providers that are designed to undermine

the openness of the Internet as a short-term measure to make extra profits.

Myth 3

Charging application and content providers will help promote broadband investment

Some access providers time and again have publicly expressed their will to charge content and application providers – in addition to access charges already paid by end-users – arguing that this will help investment in next generation networks. This is a dangerous approach because there are no existing obligations that would guarantee that access providers use any additional revenue for investment. In fact, they might even prefer to opt for less investment, since lower quality for basic Internet service may encourage the adoption of non-neutral (and more expensive) "premium" services.

Myth 4

Net Neutrality legislation isn't necessary, since customers can "vote with their feet"

If a company is restricting your access, whether blocking websites or services, the European Commission repeatedly stated that customers can switch companies to those who are offering the "full" Internet. However, if I am running a Belgian web service and it is being blocked by access providers in, say, Poland, Greece and Spain, I have no choice as I am not a customer of the foreign providers that are blocking my freedom to conduct business.

For consumers, good switching is insufficient in an industry where they are tied into lengthy contracts, as their ability to switch providers may not be feasible in practice. End-users can be left in a restricted, low quality slow lane, or a fast lane with fewer destinations to reach, without even knowing about it.

Myth 5

There is no need for regulation, let the market decide

This is a false dilemma. While competition is a necessary mechanism to construct a healthy market, it does not effectively prevent access providers from adopting non-neutral practices. The regulatory framework cannot solely rely on competition and transparency.

It is clear that competition law moves too slowly, and is demonstrably not effective in curbing the problem at hand. In light of the growing, overwhelming evidence that access providers are tampering with end-users' ability to access the Internet, relying solely on market forces will lead to the development of a multiple-tier Internet, to the detriment of citizens.

Myth 6

Costs are exploding because of data growth

This is untrue for both fixed and mobile network connections. For fixed telephony networks, traffic-related costs are a small percentage of the total connectivity incomes because they have a single line per household, so traffic growth over this segment involves no additional costs. The

question is different for cable and mobile networks because the cable and radio access network is shared by users and the costs of adding capacity are significantly higher than they are for fixed networks. However, the progress from 2G to 3G to 4G for mobile and to from EuroDOCSIS 1.x to 2.0 (and soon 3.1) for cable has lead to important reductions in the cost of carrying traffic. This means that even if costs for mobile access are higher, cost per unit is declining. In this case, not only does data traffic growth contribute to profitability for access providers, but it may contribute to lower average costs per data unit carried by the network.

Myth 7

Net Neutrality will harm innovation

It is not true that Net Neutrality would stifle innovation, quite the opposite in fact: a failure to enact Net Neutrality protections will undermine content and application providers' freedom to do business. As explained in chapter 3, a non-neutral regime would hinder innovation in content, as start-ups and smaller companies would suddenly be faced with barriers to enter the market – and uncertainty about what new barriers may be created. The innovators' freedom to impart information is therefore limited – as is their freedom to do business, being protected by the Charter of Fundamental Rights of the EU.

Myth 8

It's our network, we can do whatever we want with it

The Internet is a "truly public place" that enables a new frontier of freedom, and serves as a tool to exercise this freedom."[12] Citizens have grown to depend on the stability, openness and integrity of the Internet to exercise their fundamental rights, including their freedom of expression, access to information and freedom of association. These responsibilities are internationally recognised under the UN Framework, which acknowledges the corporate responsibility to respect human rights. Moreover, the EU Delegation to the 7th International Governance Forum (IGF) stated in 2012 that "the Internet is not just a technology or a digital market space.

Myth 9

Net Neutrality is a problem in the US, not in Europe

There is overwhelming evidence that European access providers, particularly in the mobile sector, are using technical measures to tamper with end-users' ability to access the Internet for their own commercial interests.

For example, recent findings from BEREC (the Body of European Regulators for Electronic Communications) show that this is indeed a problem in Europe, where more and more operators are restricting access to content (such as P2P sites), services (such as VoIP) and degrading the quality of Internet connections. In addition, the evidence collected through citizen platforms such as Glasnost[13] and Respect My Net[14] provides a crystal clear picture of the numerous, harmful neutrality violations already taking place in Europe.

THE SITUATION IN THE EUROPEAN UNION

WAITING FOR NET NEUTRALITY

If there are so many benefits to securing Net Neutrality, what is the situation in Europe? What is being done to protect it?

In late 2009, European legislators chose not to introduce a legal safeguard to protect Net Neutrality in the "Telecoms Package". This package obliges access providers to inform end-users about traffic management that they implement on their networks and to offer content or application providers access to their networks at "fair, reasonable and non-discriminatory conditions"[15]. Moreover, it says that national regulatory authorities shall promote the ability of end users to access and distribute information and run services and applications of their choice. However, in light of the significant body of evidence, the telecoms package has proven insufficient to efficiently safeguard Net Neutrality[16].

When Vice President Neelie Kroes took office as European Commissioner for the Digital Agenda in 2010, she stated that Net Neutrality would be a central issue on her agenda and launched a first public consultation. However, she moved away from this initial commitment, with one consultation after the other and not much action to ensure a neutral net in Europe.

In 2011, the European Data Protection Supervisor (EDPS), warned that violations of Net Neutrality could have "serious implications" for end-users' fundamental rights to privacy and data protection. The EDPS stated that "certain inspection techniques used by ISPs may indeed be highly privacy-intrusive, especially when they reveal the content of individuals' Internet communications, including emails sent or received, websites visited and files downloaded"[17].

In May 2012, after a series of consultations, the Body of European Regulators for Electronic Communications (BEREC) published its findings regarding traffic management and other practices that lead to restrictions to an open Internet in Europe. The data from the investigation revealed the increasing trend of providers to restrict access to services and applications.

On 15 October 2012, the European Commission's latest consultation on Net Neutrality officially ended. On a European level, this was the sixth public consultation on Net Neutrality since Neelie Kroes took office. Only two weeks later, the European Parliament demanded the end of the "wait and see" approach and called "on the Commission to propose legislation to ensure Net Neutrality."[18]

A supplementary unofficial consultation was conducted in autumn 2012, when European Member States and the EU institutions were preparing to participate in the World Conference on International Telecommunications 2012 (WCIT12)[19] organised by the International Telecommunication Union (ITU). The goal of the conference was a revision of the International Telecommunication Regulations (ITRs), which is a binding international treaty governing telephone, television and radio networks. The European Telecommunications Network Operators' Association (ETNO) proposed to include global Internet regulation in the ITRs and tabled an amendment that would allow operators to practice differentiated quality of service delivery as well as to establish "sending party pays" business models.[20] This proposal to globally abandon the "end to end" and Net Neutrality principles was not accepted by the European representatives in the process of revision of the ITRs.

Page 18/19: Timeline of the Net Neutrality debate in Europe in the last three years.

http://www.tiki-toki.com/timeline/entry/108784/Net-neutrality-in-Europe/

EVENT

NEELIE KROES SAYS:

22 december 2009

"We also need to ensure that (...) networks are reliable and resilient, open and neutral"

VIOLATION

T-MOBILE BLOCKS SKYPE

3 april 2010

Deutsche Telekom, parent company to T-Mobile, has announced that it plans to block access to Skype for iPhone in Germany.

EVENT

NEELIE KROES SAYS:

11 november 2010

"In the spirit of net neutrality all such content and applications should receive equal treatment." - "Any content or application that is legal and which does not cause undue congestion or otherwise harm other users or network integrity should be fully accessible."

EVENT

EDPS adopts opinion

7th October 2011

In his opinion, the EDPS has made some recommendations which include: the determination of legitimate inspection practices needed to ensure the smooth flow of traffic or carried out for security purposes; the determination of the cases when monitoring requires the users' consent (such as filtering aimed to limit access to certain applications and services, such as peer to peer); and, in such cases, the necessity of guidance regarding the application of the necessary data protection safeguards (purpose limitation, security etc).

EU PARLIAMENT

1ST EU PARLIAMENT RESOLUTION

26 Oktober 2011

"Calls further on the Commission to ensure that internet service providers do not block, discriminate against, impair or degrade the ability of any person to use a service to access, use, send, post, receive or offer any content, application or service of their choice, irrespective of source or target;

VIOLATION

EURO WATCHDOG: TELCOS ARE STRANGLING VOIP AND P2P TRAFFIC

15th March 2012

2010

EVENT

NEELIE KROES SAYS:

14 january 2010

"(...) that net neutrality is absolutely crucial.On a personal note I put even a heart by this item on my paper! It is of high importance for both of us, the Commission as well, to preserve the open and neutral character of the net."

VIOLATION

BT THROTTLES BBC IPLAYER

1 june 2010

BT Broadband cuts the speed users can watch video services like the BBC iPlayer and YouTube at peak times.

CONSULTATION

1ST EU COMMISSION CONSULTATION LAUNCHED

30rd June 2010

2011

VIOLATION

KPN ANNOUNCES USE OF DPI

22 april 2011

Dutch mobile provider KPN announced plans to charge mobile phone users separate fees for using voice-over-IP (VoIP) services like Skype, instant messaging programs, and streaming video.

VIOLATION

FRENCH ISP THROTTLES YOUTUBE

3rd May 2011

CONSULTATION

1ST BEREC CONSULTATION LAUCHED

15th October 2011

The BEREC launches a consultation on its guidelines on Net Neutrality and Transparency

EVENT

NEELIE KROES SAYS:

9th November 2011

she heard "allegations that some internet providers throttle, degrade the quality of services"

2012

CONSULTATION

2, 3 & 4 BEREC CONSULTATIONS LAUNCHED

23rd February 2012

BEREC launches consultations - three guidelines on Quality of Service (BoR 32), IP-interconnection (BoR 33) and differentiation practices (BoR 31)

EVENT

NETHERLANDS ADOPT LEGISLATION

8th May 2012

In reaction to KPN's anti-neutrality plans, a broad majority in the Dutch Parliament voted for a legislative proposal to safeguard an open Internet in The Netherlands.

EVENT

NEELIE KROES SAYS:

29th May 2012

"consumers also need to know if they are getting Champagne or lesser sparkling wine. (...) I do not propose to force each and every operator to provide full Internet."

STUDY

BEREC publishes findings

29th May 2012

"At least 20% of mobile Internet users in Europe have some form of restriction on their ability to access VoIP services (...)"

EU PARLIAMENT

EU PARLIAMENT DEMANDS NET NEUTRALITY - AGAIN

15th December 2012

EU Parliament demands stronger net neutrality protections - the resolution "Digital Freedom Strategy in EU Foreign Policy", stresses that the EP "strongly supports the principle of net neutrality, namely that Internet Service Providers do not block, discriminate against, impair or degrade, including through price, the ability of any person to use a service to access, use, send, post, receive or offer any content, application or service of their choice, irrespective of source or target" and "calls on the Commission and Council to promote and preserve high standards of digital freedom in the EU, in particular by codifying the principle of net neutrality.

CONSULTATION

2ND COMMISSION CONSULTATION LAUNCHED

23rd July 2012

A new Net Neutrality EC consultation delays possible regulations

EU PARLIAMENT

EU PARLIAMENT DEMANDS NET NEUTRALITY LEGISLATION

26 Oktober 2012

"81. Calls on the Commission to propose legislation to ensure net neutrality;"

EVENT

SLOVENIA INTRODUCES LEGISLATION

20th December 2012

2013

VIOLATION

ORANGE MAKES GOOGLE PAY FOR TRAFFIC

16th January 2013

VIOLATION

VODAFONE BLOCKS VIBER

26th February 2013

STUDY

Commission group recommends legislation

23rd January 2013

"Channels or mechanisms through which media are delivered to the end user should be entirely neutral in their handling of this content. In the case of digital networks, Net Neutrality and the end-to-end principle should be enshrined within EU law."

EVENT

NEELIE KROES SAYS:

20th March 2013

"I'm fed up hearing from people who cannot legally access the music and films they love; from artists who can't reach the audiences they want; from scientists who can't properly use modern research techniques."

VIOLATION

FRANCE: SFR VIOLATES NET NEUTRALTIY

30th March 2013

SFR violates net neutrality by modifying HTML content on internet mobile.

EVENT

LEAK: DRAFT REGULATION FOR A "TELECOMS SINGLE MARKET"

11th July 2013

The leaked regulation aims, in Article 20, to prohibit anti-competitive blocking and throttling, BUT at the same time it proposes also the exact contrary of guaranteeing net neutrality by explicitly allowing agreements between content and access providers to prioritise traffic.

EVENT

NEELIE KROES SAYS:

11th July 2013

"So I will guarantee net neutrality. (...) Allowing the new premium services which so many new services rely on"

THE NETHERLANDS: A CASE STUDY

Contribution by Bits of Freedom

A CASE STUDY

In 2011, the former Dutch telecoms monopolist KPN announced plans to make users pay extra for data used by certain third-party applications, such as WhatsApp and Skype, in order to create an advantage for KPN's own services that included text messaging and phone calls. In May 2011, KPN revealed that it had used Deep Packet Inspection (DPI – see box on page 9) technology to identify the use of certain applications by its mobile Internet customers[21].

One year later, on 8 May 2012, the Netherlands adopted crucial legislation to safeguard the open and secure Internet, including Net Neutrality provisions.[22] By doing so, the Netherlands is the first country in Europe and the second country in the world to enshrine the principle of Net Neutrality in law. This demonstrates that it is possible to draft Net Neutrality legislation that takes into account the interests of Internet users, service providers and telecommunication companies, while ensuring freedom of expression and privacy on the Internet.

The law aims to maximise choice and freedom of expression on the Internet. It therefore prohibits the hindering or disrupting of services or applications on the Internet. Only in certain limited cases where this is necessary is an exception to this principle allowed. Those exceptions must be interpreted narrowly, whereby the assessment of the necessity must be based on the criteria of proportionality, using criteria established in the context of the application of the European Convention on Human Rights.

The first exception aims to ensure that in case of congestion, time-sensitive traffic (such as VoIP) can be prioritised, and that in such cases other traffic may be delayed. Providers should avoid congestion in the first place by adequate investment in capacity. However, if there is congestion, then the measures under this exemption are designed to facilitate end-users' ability to continue to have maximum access to information, disseminate information and use applications or services. The measures should be removed as soon as possible.

The second exception is aimed at blocking

traffic that affects the safety or integrity of the network or of the end-user's terminal device. This can, for example, be traffic from computers that are part of a botnet and which is used for a distributed denial of service attack. A measure must be proportionate and therefore must be restricted to only the traffic that affects security or integrity, and should be used no longer than necessary.

The third exception is designed to make it possible to block unsolicited commercial communications such as spam.

Finally, an exception allows for the situation where providers are required by statute to hinder or slow down certain traffic, or are required to do so under a court order.

In addition, providers of Internet access services are not allowed to make the price of Internet access services dependent on the services and applications which are offered or used by customers.

"As much as anything else, the economic success of the Internet comes from its architecture."

- Lawrence Lessig, Harvard Law School Professor [23]

TEN POINTS TO SAFEGUARD NET NEUTRALITY

1 The Internet must be kept neutral and open.

2 Accessibility between all endpoints connected to the Internet without any form of restriction must continue to be upheld.

3 All forms of discriminatory traffic management, such as blocking or throttling should be prohibited, unless as part of objectively necessary traffic management measures.

4 Traffic management should only be allowed as a narrowly targeted deviation from the rule. It must be either necessary, proportionate and legally required, or required to address a transient network management problem which cannot be dealt with otherwise.

5 Legal clarity must be established to determine what types of traffic management are legitimate under which circumstances.

6 Access providers have to indicate in their contracts and advertisements a guaranteed minimum bandwidth, maximum latency and quality measures for the connection (so that customers can determine whether a particular connection can e.g. be used with Skype). Access providers have to provide tools to verify those standards. These standards must be determined with a statistical method that has to be published.

7 We need to establish a clear set of obligations for access providers regarding the neutrality and best effort of the Internet broadband services on the one hand, and for specialised services that are not transported via the Internet on the other.

8 By default, only header information should be used for traffic management. The use of deep packet inspection (DPI) should be reviewed by national Data Protection Authorities (DPAs) to assess compliance with the EU's data protection and fundamental rights framework.

9 End-users should be able to report violations of the points above to an authority defined by the government. This authority must have the necessary resources to enforce the above conditions.

10 EU-wide legislation on Net Neutrality should provide for financial sanctions with a sufficient dissuasive effect.

GLOSSARY

Best effort The Internet operates on a "best effort" basis in contrast to the telecoms world's end-to-end voice circuit with a guaranteed Quality of Service. This is because data traffic is often short and bursty and the overhead involved in trying to reserve resources in advance for such traffic would often be wildly excessive. In addition, there are simply too many networks involved in the Internet to allow all the direct contractual relationships that would be needed for generalised QoS. See also peering.

DOCSIS DOCSIS is an international telecommunications standard that permits the addition of high-speed data transfer to an existing cable TV system.

End-to-end principle The end-to-end principle is part of the Internet's core architecture. This principle asserts that Internet communications should be controlled at its endpoints rather than by intermediaries. The "transmission pipe" does not discriminate against the sender, recipient or content of the data transmitted over the network.

Filtering The act of blocking specific packets of data when they travel through networks based on pre-defined criteria. It can be used as a technique to implement security firewalls but also to censor communications.

IP (Internet Protocol) IP is a communications standard that allows computers to send data packets to one another. IP is the basic communication technology of the Internet.

IP address An IP address is a numerical address that is assigned to every device connected to the Internet (check our booklet "How the Internet Works"). As household or business routers will often display just one IP address for all of the people connected to it, the IP address can identify a group of people rather than just one individual.

Internet access provider An access provider is a company that offers access to the Internet, that operate fixed/mobile infrastructure or provide access to infrastructure.

ISP (Internet Service Provider) ISP is the general term for companies or organisations that provide access to the Internet and related services. There are different types of ISPs, such as access, hosting, virtual and transit providers.

Peering Many networks on the Internet swap traffic with their peers without payment. This is a sophisticated response to a complex environment. Accounting and billing and even negotiating the contracts in the first place involve costs for any organisation. At its simplest, your access provider's network is paid for by its subscribers. It may then buy bulk transit to access the rest of the Internet. But if it can then simply swap traffic with its peers then this can be win-win for all concerned. It would be illogical to pay your peer when they will just have to pay you back - and in addition you would both need to assume the costs of all the overheads of such an arrangement.

Peer to peer (P2P) A decentralised system where the end-users ("peers") are connected directly with each other via the Internet.

Throttling Throttling means the intentional slowing down of services, applications or content by an Internet access provider.

Transmission Control Protocol (TCP) TCP is the protocol responsible for verifying the correct delivery of data and keeping track of data packets. TCP helps to detect errors and to trigger retransmission until the packets are correctly and completely received.

TCP/IP architecture TCP and IP are the most common as well as the oldest standards for Internet communication. As most transmissions of data across the Internet take place using TCP on top of IP, the name TCP/IP has come to represent the complete suite of protocols used on the Internet. These protocols define the rules that computers must follow in order to communicate with each other and send data to the right destination.

Traffic management ISPs have always engaged applied mechanisms to control traffic flows to preserve the security of the network or to avoid congestion. If ISPs engage in supplementary practices (in addition to the existing congestion control by TCP/IP) to inspect and to differentiate traffic, this is often referred to as "traffic management".

VoIP (Voice over IP) A set of data communications protocols and technologies to enable voice to be sent over the Internet or over separate, IP-based networks.

Notes

01 http://www.commerce.senate.gov/pdf/cerf-020706.pdf

02 EDRi booklet: How the Internet works http://www.edri.org/files/2012EDRiPapers/how_the_internet_works.pdf

03 http://europa.eu/rapid/press-release_SPEECH-08-473_en.htm

04 Open Rights Group: http://www.openrightsgroup.org/blog/2012/peace-advocates-blocked-as-porn

05 BBC: Virgin defends file-sharing campaign http://news.bbc.co.uk/newsbeat/hi/technology/newsid_7486000/7486836.stm and Virgin Media and Cview to rifle through your packets: http://crave.cnet.co.uk/software/virgin-media-and-cview-to-rifle-through-your-packets-49304424/

06 Open Net Initiative, West Censoring East https://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011

07 Wired, The Kremlin's New Internet Surveillance Plan, 1 November 2012: http://www.wired.com/dangerroom/2012/11/russia-surveillance/all/

08 Thomas Grob, Deutsche Telekom, at the Netz-für-alle-Konferenz: https://www.youtube.com/watch?v=HQbwiZ5hIoo#t=20m28s

09 BEREC report on traffic management, 2012: "When blocking/throttling is implemented in the network, it is typically done through deep packet inspection (DPI)" https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf

10 European Parliament resolution, 26/10/2012 http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2012-0341&language=EN

11 PLUM study 2011 http://skypeblogs.files.wordpress.com/2011/10/plum_october2011_the_open_internet_-_a_platform_for_growth.pdf

12 Joint Statement of the EU Delegation to the 7th International Governance Forum (IGF) in Baku http://europa.eu/rapid/press-release_MEMO-12-852_en.htm

13 Glasnost data visualised in a Net Neutrality map http://netneutralitymap.org/

14 Respect my net: http://respectmynet.eu/list/

15 Directive 2002/19/19 (Access Directive): http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0019:EN:HTML

16 See BEREC study May 2012 http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf

17 EDPS Opinion on Net Neutrality, traffic management and the protection of privacy https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2011/EDPS-2011-10-Net-neutrality_EN.pdf

18 EU Parliament resolution on completing the Digital Single Market, 26 October 2012: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2012-0341&language=EN

19 See WCIT resources: http://wcitleaks.org/resources/

20 ENDitorial: The ETNO's WCIT Proposals are not as bad as some say http://www.edri.org/edrigram/number10.19/wcit-etno-proposals-not-so-bad

21 Web wereld: KPN luistert abonnees af met Deep Packet Inspection http://webwereld.nl/beveiliging/53691-kpn-luistert-abonnees-af-met-deep-packet-inspection

22 The translated provisions can be found on the website of Bits of Freedom: https://www.bof.nl/2011/06/27/translations-of-key-dutch-internet-freedom-provisions/

23 http://www.nytimes.com/roomfordebate/2010/8/9/who-gets-priority-on-the-web/a-deregulation-debacle-for-the-internet

EDRI.ORG/PAPERS

With financial support from the EU's Fundamental Rights and Citizenship Programme.