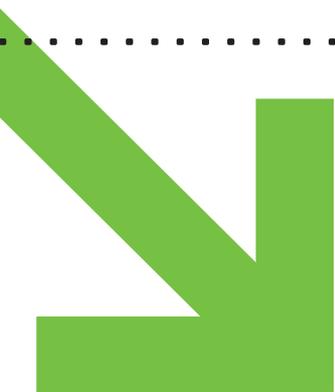

Q&A

ON NETWORK DISCRIMINATION IN EUROPE



WHY EUROPE NEEDS NETWORK NEUTRALITY LEGISLATION

WHAT IS NETWORK DISCRIMINATION?

Network discrimination is the practice of many Internet Service Providers (ISPs), including telecommunications and mobile network operators – who control almost all private internet access – of putting arbitrary restrictions on the free and open internet. Generally speaking, network discrimination can take place in different ways:

BLOCKING APPLICATIONS AND SERVICES

In order to maximise profits, some ISPs exclude certain services and applications of competing market players. The most prominent case regarding this form of network discrimination is European mobile network operators (like [Deutsche Telekom](#)¹) blocking or restricting Voice over IP (VoIP) services (like Skype and Viber) for users on their network.



SLOWING OR THROTTLING INTERNET SPEEDS

Some ISPs slow down specific services (like Spotify) and applications (like Skype), or ask users to pay an extra fee to have access to these internet platforms.



BLOCKING WEBSITES

ISPs often block websites for a number of reasons. In the UK for example, [Orange Telecom](#)² blocked the French digital rights advocacy group, La Quadrature du Net's website on pre-paid mobile accounts.



DATA CAPS

Some ISPs charge users depending on how much data they upload and download. This is increasingly used as a way of providing preferential access to certain services, thereby undermining competition and innovation. For instance, [Deutsche Telekom](#)³ now imposes strict data caps on internet access contracts, but the company's own streaming services, "T-Entertain", does not count against this data allowance. Furthermore, Spotify – the popular music streaming service – is favoured ahead of its competitors, effectively limiting the market for legal online music.

HOW ARE THESE PRACTICES JUSTIFIED?

Many ISPs claim that the exponential growth in web usage, particularly bandwidth intensive video applications, along with the alleged rise in infrastructure costs, mean that their networks are

congested and that without a degree of traffic management, congestion would make it impossible for users to enjoy sufficient quality of service. Therefore, ISPs insist that they should be allowed to prioritise some packets over others in order to provide “guaranteed quality of service” for some applications compared to others.

While ISPs should be able to manage their networks so that bandwidth is available to meet all the needs of most users, traditional traffic management does not include arbitrary restrictions by network operators, as these practices go clearly against the “best-effort” principle that is fundamental to the the internet’s functioning.

No.3

HOW DOES THIS UNDERMINE THE BASIC FUNCTIONING OF THE INTERNET?

Network discrimination risks destroying the two principles that have made the internet the success it is today, namely, the the best-effort principle and the end-to-end principle.

First, imagine the internet as a set of boxes (i.e. routers) connected by long wires (i.e. links) that allow internet messages (data packets) to be forwarded from a box to another until it arrives at its destination.

THE BEST-EFFORT PRINCIPLE

Due to the best-effort principle⁴, if one of the destination boxes is full or busy, the incoming messages are delayed and have to wait for delivery. Following the best-effort principle, the internet

will do its best to deliver each message promptly and make sure that all messages are treated equally, independent of their source, destination, or content.

Assigning priorities on the basis of business priorities goes against the neutral best-effort principle.

THE END-TO-END PRINCIPLE

According to the end-to-end principle, the ISPs’ main purpose is to move the information from any end-point (user) to another, without interfering with the contents of that message.

If a website is blocked, a connection from one user to another is no longer possible, thereby undermining the end-to-end principle.

No.4

HOW CAN WE ENSURE THAT THE INTERNET REMAINS OPEN AND FREE?

Through the enforcement of the network neutrality principle.

Network neutrality is the guiding principle that preserves the very essence of the internet, its openness and free accessibility. According to this principle - except for limited exceptions such as spam and viruses - the companies that deliver information over the internet should treat all content equally, delivering each package of information as quickly and efficiently as possible. This equality is exactly what has made the internet an open platform and the generator of innovative ideas, value creation, effective competition, and promoter of freedom of expression.

4. <http://bit.ly/10TqtXg>

No.5

WHY DO WE NEED NETWORK NEUTRALITY?

If enshrined into law, network neutrality would guarantee that ISPs do not discriminate between different kinds of content and applications online.

It would also ensure the free flow of content, open access to sites and platforms, and would thereby guarantee democratic participation, competition, and freedom of expression online.

Furthermore, network neutrality drives economic innovation. Many of today's most successful applications were able to develop because of the existence of a neutral playing field allowed them to flourish alongside other more dominant, pre-existing players. Therefore, a departure from network neutrality will hinder innovation and impede the emergence of new start-ups in the EU.

No.6

IS NETWORK DISCRIMINATION A PROBLEM IN EUROPE?

In May 2012, the Body of European Regulators for Electronic Communications (BEREC) published the findings in a joint investigation with the European Commission regarding [traffic management](#)⁵.

It revealed an increased trend of operators restricting access to services and sites. The most frequently reported restrictions are the blocking and/or throttling of peer-to-peer (P2P) traffic, on both fixed and mobile networks, and the blocking of Voice over IP (VoIP) traffic, mostly on mobile networks.

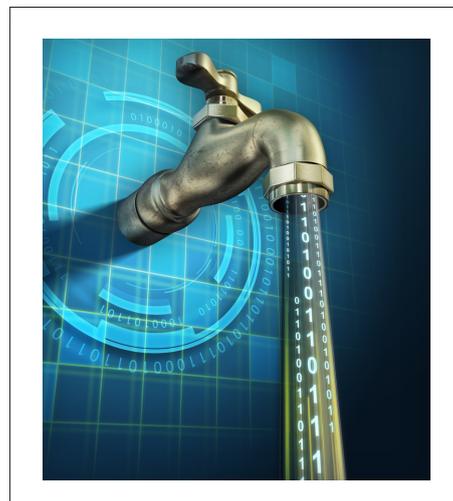
No.7

WHAT ARE POLICY MAKERS DOING TO FACE THIS PROBLEM?

Not enough.

In the Summer of 2010 the European Commission launched a public consultation on "[The open Internet and net neutrality in Europe](#)"⁶ to delve into issues of internet traffic management. Since then, five more consultations have been launched, but no concrete actions have been undertaken in order to preserve the internet's neutral infrastructure. The Commission is delaying, continuing a "wait and see" approach, which neglects the urgent need for regulatory measures.

The Commission plans to publish its Recommendations on the Open Internet and Net Neutrality by the end of 2013. However, a recent [blogpost](#)⁷ from Commissioner of the Digital Agenda Neelie Kroes highlights that the Commission has abandoned its commitment to network neutrality. Kroes' focus is on ensuring that companies are transparent about "what type of internet they are offering - whether a "champagne" or "lesser sparkling wine" internet - which is an alarming scenario for the preservation of the network neutrality principle in Europe.



5. <http://bit.ly/VDHK0y> 6. <http://bit.ly/ckvY7d> 7. <http://bit.ly/KpRofE>

In reality, the internet is not a luxury like champagne, it's as critical to life these days as water. The United Nations have acknowledged this reality and recently declared that access to the internet, much like water, is a basic human right⁸.

Given the many implications of network discrimination, "wait and see" is not enough to preserve the open internet - legislation is needed!

No.8

ARE THERE COUNTRIES PROTECTING NETWORK NEUTRALITY IN LAW?

In 2011, the Netherlands⁹ became the first country in Europe and second country in the world after Chile¹⁰, to require that internet service providers abide by the Net Neutrality principle. Soon after, in December 2012, Slovenia¹¹ followed, adopting a legislative framework protecting Net Neutrality.

These laws, although with some differences, would not only prohibit providers from throttling or filtering the connections of their customers but, in the case of the Netherlands, providers would also be prevented from using deep packet inspection¹² (DPI) -- which can be used as an advanced surveillance tool -- to spy on their customers without their express consent or a legal warrant.

No.9

IS THERE DISCRIMINATION ON MY NETWORK?

Companies aren't always transparent about restrictions they may implement on your internet connection. The best way to find out is to go on your mobile operator's website and check your tariff plan.

If the Terms and Conditions state that the offer does not include the use of VoIP and P2P, it means that you will not be able to use applications such as Skype or Viber to call your friends or listen to your favourite music on Spotify!

No.10

WHAT CAN I DO?

- >> Have you been subject to network discrimination? Would you be willing to pay extra to have "champagne" access to the internet? Let us know at [Brussels@accessnow.org!](mailto:Brussels@accessnow.org)
- >> Retrace the history of Net Neutrality in Europe through a timeline¹³ created by European Digital Rights (EDRi).
- >> Check out our website¹⁴ where you can find more information and updates on network discrimination in Europe.

8. <http://bit.ly/is08oq> 9. <http://bit.ly/K10lXD> 10. <http://bit.ly/13K0tXx> 11. <http://bit.ly/TyclZs>

12. <http://bit.ly/J6LpdZ> 13. <http://bit.ly/18hMTNT> 14. <http://bit.ly/14x2Qhy>