EUROPEAN
DIGITAL
RIGHTS

Net Neutrality Conference, Bucharest, 05 June 2012

First of all, thank you to ANCOM and ApTI for organising this event and for inviting European Digital Rights to speak to you today on Net Neutrality. EDRi is an association of 32 digital civil rights organisations from 20 European countries and the neutral, free and open Internet is clearly one of our biggest concerns.

The Internet was created with an architecture that is open, neutral and minimalist. This has made the Internet so robust, so flexible and so successful – on a social, technical and economic level. We must now ensure that it is passed on to future generations.

Last December, European Commissioner Kroes said that the Arab Spring has been “a wake-up call” to increase the positive role of technology in the spread of democracy.

In the open and neutral Internet, users can all freely communicate, fully express themselves, access information and participate in the public debate - without unnecessary interference by gatekeepers or middlemen. It is a “single market” for communication and for business – the kind of borderless market that Europe has been trying to build for decades.

This principle is an important safeguard against censorship and protectionism, both by public and private actors, and it thereby helps ensuring a functioning democracy and economy. This is what we have to keep in mind when we discuss net neutrality.

However, the safeguards that have allowed Internet services and applications to flourish are under growing assault. We know the value of the open Internet for society and for the economy. What is less clear in the public mind is just how many experiments are being proposed and undertaken that are putting this value at risk. And yes, to answer straight away the first question of this panel: The very nature of the Internet is affected by unnecessary traffic restrictions and limitations.

In this short presentation, I will try to briefly sketch out the shape of the current threats. First, I will look at government demands for interferences in Internet traffic, and second at commercial and, ultimately, anti-competitive, interferences.

1. **Government demands for interference in traffic**

The EU Telecoms Package from 2002 says that national regulatory authorities shall promote the freedom to access and distribute information, to run services and applications of our choice. This is the freedom of access to the Internet – and this simple rule means that there is only one Internet for everyone – and that everyone can participate.

For example, if you are in China you can only access or distribute some specific information and not all information of your choice. And this is not the Internet, it's the “Chinternet”. In Iran, they call it “clean” or “halal” Internet.

But also western governments are more and more often 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 around forty. In Europe, website blocking has been introduced for instance in Belgium, France, Italy, in the UK and in Ireland.

Italy's web blocking scheme grew to a situation where it is used for an ever-growing range of content: In July 2011, almost 5000 sites were already being blocked. And this is now undermining the rule of law since the Italian system allows to block sites even in the absence of a court order.

In the UK, mobile operators have introduced a filtering tool to prevent viewing of perfectly legal adult-related content – a practice which has already led to the accidental blocking of websites of civil liberties groups and peace advocates.

Over the past years, many western governments have done "behind-the-scenes" efforts to persuade, or reward Internet companies into developing censorship structures. Our governments, and the EU Commission, call this "self-regulation" and demand that Internet providers take more responsibility for illegal online activity. The purpose of this is to hand over judicial responsibilities to private companies.

Companies implementing such privatised enforcement measures are of course less bound by the obligations imposed on courts. This action can be, for instance, to have payments blocked by payment providers, search results deleted by search engines, websites blocked or Internet traffic filtered by providers – all these practices are slowly eroding the rule of law.

Even though western governments must respect their constitutions, life just becomes much simpler for them when private companies can take extra-judicial action against unwelcome online information.

This trend for governments to outsource regulation of the Internet is happening at a moment when Internet companies are increasingly open to such requests. And this leads me to the second point:

2. **Private sector interference and network management**

Anti-net neutrality companies are campaigning for the right to interfere in Internet traffic for their own commercial purposes. The most notable example of discrimination involved the Deutsche Telekom's, or rather T-Mobile's, blocking of Voice over IP, provided by Skype. Kabel Deutschland, a German access provider, is known for its practices to throttle file sharing traffic.

So whenever mobile and fixed access providers tell us in their Terms and Conditions, that we cannot use P2P or Voice over IP, this is not the Internet either. Maybe you can call this “Orangenet” or “Vodafonenet”, but not the “Internet”. This is a serious threat to fundamental rights, and a restriction of our freedom of expression - by restricting access.

Some politicians now call for net neutrality and at the same time demand filtering or blocking for law enforcement purposes. But it is simply a paradox to create legal incentives for ISPs to invest in monitoring and filtering/blocking technology, while at the same time, demanding that ISPs do not use this technology for their own business purposes.

For instance, Virgin Media provides access to the Internet and is increasingly using Deep Packet Inspection (DPI). DPI is a very privacy-invasive technology which enables providers to look into the contents of data sent to or received from their consumers. Virgin is now using this technology to police possible copyright infringements that would undermine its music business.

In the Netherlands, the use of Deep Packet Inspection by the ISP KPN has caused such an outrage that the country has now become the first European Member State to enshrine Net Neutrality in law.

Vint Cerf, one of the Internet's founding fathers, explained that “Allowing broadband carriers to control what people see and do online would fundamentally undermine the principles that have made the Internet such a success”.

But providers often argue that open-access requirements would destroy their incentive to build fast, new networks. But real-world experience shows that this is not true. Access providers also argue that competition law will solve all problems. But real-world experience shows that ex ante regulation is indispensable.

The vibrant Internet access market in France, for instance, did not happen spontaneously.
About a decade ago, the government forced France Telecom to lease capacity on its wires to rivals for a regulated price, allowing competitors to storm in.

This regulation was fiercely opposed by France Telecom at the time. But it has proven to be massively beneficial not just for French citizens, not just for competitive operators but for France Telecom itself, as it is now leaner, fitter and more competitive than it would ever have been in a closed, ill-functioning market.

This example clearly shows that enforced competition is the only way to ensure healthy network markets.

In short, unnecessary network management by access providers restricts the freedom of expression of end-users and the fundamental freedom of other service providers, and entrants to the market, to conduct business.

The neutral architecture of the Internet and its devices has permitted innovative start-ups to grow – Let's take Google, Wikipedia for example: It would be much more difficult to start such companies without an open and neutral net. This is the core of the contradiction between wider economic needs and a non-neutral Internet.

To conclude,

if we have understood that new technologies and digital media can be an effective tool for political expression, we now need to move to the urgent question of how digital technology can be kept free and open.

How do we ensure that the Internet remains neutral, and how do we avoid unnecessary traffic management? The answer is that we need EU-wide legislation to ensure network neutrality, that we enshrine this important safeguard against censorship, both by public and private actors, into law.

Only last week, European Commissioner Kroes has proposed to draft recommendations to ensure that consumers have a choice – but is this really enough for net neutrality in Europe?

Unless individual governments or the European institutions act soon — our freedom to access and distribute content on the Internet will be artificially limited. Giving consumers the choice between several bad options is not an option. We need legislation to safeguard the open, neutral and thereby sustainable Internet.