Net neutrality vs traffic management policies

A briefing paper on the Telecoms Package Second Reading

Abstract

This paper argues that subtle amendments proposed in European telecommunications law (known as the Telecoms Package) could represent major changes for the Internet and radically alter its open character, with major consequences for citizens, businesses and innovation.

More precisely, it considers how new technology available to the network operators - referred to as "traffic management systems" - will enable operators to leverage control over their networks to set priorities for content, applications and services, and discriminate between them.

We demonstrate that certain Telecoms Package amendments could *de facto* give network operators the right discriminate, while minimal power is given to regulators to deal with any abusive practices.

We consider the case of Comcast addressed by the FCC in the US, and whether a European regulator would have sufficient power to take action if a similar case occurred in Europe.

The paper concludes by arguing that the principle of open architecture in communications networks needs to be reaffirmed once again and a deeper appreciation of its importance remains crucial and should be defended in European policy debates.

Furthermore, this paper maintains that a stronger role of national and pan-european regulators in overseeing and monitoring discriminatory practices by network operators is becoming crucial.

Net neutrality vs traffic management policies

"It might be hard to see how the principles of network design could matter much to issues of public policy"

Lawrence Lessig, The Future of Ideas (2001)

The Telecoms Package, currently in the Second Reading of the European Parliament, proposes changes to the rules which govern the telecommunications industry – amendments which are on the surface subtle, yet in practice are radical. They are subtle because the wording - which suggests that network operators should be permitted to manage their networks without interference - sounds reasonable, logical and innocuous. However, when one fully understands the context of these words, it's the most radical change in almost 20 years of the public Internet's existence .

The specific changes are wrapped up in a series of amendments to the Universal Services directive (Directive 2002/22/EC), such as Article 22.3[i] of the Council's Common Position, linked with European Parliament proposed amendments to the Universal Services Directive (5, 9, 43, 49 and 53) and to the Access directive (85, 90) and Authorisation directive (107). These amendments, which introduce the notion of "traffic management policies" and 'limitations' on use of the Internet, propose to permit network operators to implement discriminatory practices against users and content providers, with minimal tools given to the regulators to deal with abusive practices. Combined with the e-Privacy directive, Article 6.7[ii] they could permit wide scale filtering of Internet services, applications and content in Europe.

Echoing Lessig's words, here we have public policy giving its blessing to a total revamp of network design principles. The essence of the radical change is that network operators will be permitted to do something they are currently not permitted to do with Internet traffic - to use new technologies to discriminate between different types of content, applications and services. This is a fundamental change in the design of the Internet, which was built on a principle of *neutrality* – a design principle that was deliberately chosen by its founding fathers.

The reason why such a design change matters to public policy is that it will have implications for innovation, for industry and for users. The principle of network neutrality has protected freedom of content and innovation since the birth of the Internet. It empowers citizens and businesses. If we allow network operators to discriminate on network traffic, to privilege certain services over others, to prioritize particular clients over others, we can say goodbye to the benefits of the open the internet as we know it. Public policy must therefore take account of the potential for abusive practices and ensure that the regulatory bodies have the tools to deal with the types of situations that could arise, in order to protect citizens. In this respect, regulators should not constrained from acting in cases where users and citizens are disadvantaged by the network operators' practices.

Why the neutrality of the network is important

It was just at the end of the 1990s, that Lawrence Lessig warned how much the architecture of the network matters. He was referring to the crucial quality of network's architecture that implies placing intelligence at the ends and keeping the middle part – the transmission – as free as possible. Thus, the Internet as it is today, is based on a principle of non-discrimination. At a technical - transmission - level, all data travels from A to B without interference. The network is neutral, it cannot discriminate between one type of data and another. This is known as the end-to -end principle. Lessig and McChesney, in their article '*No Tolls on the Internet*', claim that it is our duty to preserve its neutrality: "Net neutrality means simply that all like Internet content must be treated alike and move at the same speed over the network. The owners of the Internet's wires cannot discriminate. This is the simple but brilliant "end-to-end" design of the Internet that has made it such a powerful force for economic and social good." [iii]

Similarly, the data is carried independently of the originator, of the content or media, or protocol[iv]" Access to content and data is independent of the network, which merely provides the connection and the means of transit, but does not choose what is available. For example, what most of us know as 'the Internet' is in fact, the World Wide Web (WWW). The WWW allows us use to view, read and download text, images, and audio-visual material on computers all around the world. It is the WWW which opened up opportunities for, innovation ,trade, and knowledge-sharing. In the seminal book "*The future of ideas*" Lessig (2001) explains how the invention of the World Wide Web by Tim Berners-Lee would not have been possible without the neutrality of the network. The WWW is merely a set of protocols for displaying hyperlinked documents linked across the internet (ibid :41). People were able to deploy the WWW because the network couldn't discriminate and therefore they didn't need to ask permission from the owners of the network, or the owners of the computer systems. "I designed the web so that there should be no centralised place where someone would have to 'register' a new server, or get approval for its contents" (Tim Berners-Lee quoted in Lessig, (2001) p44). .

In the context of the Telecoms Package amendments, the comments of Stanford academic Mark Cooper (2004) are especially relevant. Public policy needs to protect *all* layers of the network, from the physical infrastructure to the content and applications which run on top: “the physical layer of facilities (the infrastructure ofcommunications) must remain accessible to consumers and citizens, for it is the most fundamental layer in which to ensure equitable access to the rest of the communications platform. An open communications platform promotes a dynamic space for economic innovation and a robust forum for democratic discourse. The role of regulation should be to ensure that strategically placed actors (perhaps by historical favor) cannot deter expression or innovation at any layer of the platform. This is best achieved by mandating that the core infrastructure of the communications platform remain open and accessible to all” (Cooper :2004:144)[v]

In Europe, these ideas have been backed by the Information Society Commissioner Viviane Reding, who stood up in favour of neutrality principle *“"Net Neutrality" has to be guaranteed”* as does the open character of the Internet*:* *“we will only be able to reap the full social and economic benefits of a fast moving technological landscape if we manage to safeguard the openness of the Internet. Openness is one of the key ingredients that made the Internet so successful as an innovation place, and we have to make sure that it is not compromised.”* [vi]

In dealing with the concept of net neutrality, it can be helpful to consider the analogy of driving a car on a public road.[vii] Once the car-owners have paid their road tax, they are free to go anywhere. But what if every car had to register with a grid before it could begin a journey? What if the grid could monitor everywhere we go, store our data and years later find out where we went? Our freedom of movement is guaranteed by law, and is a fundamental principle of a democratic, open and free society. Also, it empowers users and businesses. Now that more of our lives are being conducted online, it is important to retain the same principles in the online world.

Traffic management policies: how the open Internet can be undermined

Net neutrality is not, as some would argue, a solution looking for a problem. The problem is already with us. And nor is it merely a competition issue, as is also argued. Or even a US issue that doesn’t affect Europe. It’s true that there has been more debate about network neutrality in the US, but it’s also the case that, as with everything in high-technology, the US generally gets it first.

The reason relates to developments in network management technologies. When the commercial Internet began in 1991[viii], the technology to interfere with users’ traffic on a wide scale did not exist. In the last five or so years, however, we have seen the introduction of technology which can automate the checking, prioritisation, and redirection of Internet content as it is transmitted down the networks. This technology is known as “traffic management” or “traffic shaping” . It uses a technique that is known as deep packet inspection.

The intention of “traffic shaping” is that it allows network operators more flexibility in managing network traffic in periods of congestion. The effect however, is that by permitting prioritisation of certain types of traffic, it opens the door for discrimination between different types of traffic, and offers them the possibility to either prioritise or degrade, restrict or block traffic on behalf of particular content providers, or in favour of particular applications.[ix] This is also known as network filtering.

Using deep packet inspection, the network operator can look into the data packets to see what users are sending, and make decisions on how to direct their communications based on the content of the packets. This is the equivalent of the post-office opening every envelope and making a forwarding decision based, not on the address, but on the contents[x]. For example, peer-to-peer traffic can be restricted. If “cooperation” between rights-holders and ISPs is “promoted”, as in Article 33(3) of Universal Services Directive (Council’s Common Position)[xi], we could foresee a scenario where such restriction would be put in place to support copyright enforcement.

Traffic management systems act on rules that are placed in the database which controls them. These rules are known as the ‘policies’ and they may be general ones for groups of users, or individual policies for single users. Such *traffic management policies* can be set to support any requirement whether political or commercial.In Europe, these policies are currently set according to the business plans of the network operators. In China, the these policies operate on behalf of political censorship. However, they can be programmed to operate on behalf of any interest group, state or private. In such a scenario, traffic management becomes more like an automated policeman or censor, and from a policy-makers viewpoint, that is that risk that we should seek to protect against.

Commissioner Reding has expressed her concerns about “traffic management policies”*: “ New network management techniques allow traffic prioritisation. These tools may be used to guarantee good quality of service but could also be used for anti-competitive practice, she said.”*[xii]In the US, the FCC has already ruled against abusive network management policies. In August 2008, the Federal Communications Commission (FCC) made an order against the network operator Comcast. The effect of the ruling is that network operators cannot filter peer-to-peer traffic, or indeed, they can’t pick on any specific type of traffic and filter or slow it down or ‘restrict’ it. The FCC ruling was made against the network operator, Comcast. The FCC said that Comcast’s network management practices, which involved slowing down and restricting access to peer-to-peer services, were anti-competitive and discriminatory.

The FCC has recognised that network operators should not use the veil of "traffic management" to block or slow down their customers' traffic, or to selectively discriminate between applications and services, rather than treat all equally, and to attempt to cripple competitive services. It also reiterated that consumers have the right "*to go where they want, when they want, and generally use the Internet in any legal means*". FCC chairman Kevin J Martin said in his press statement[xiii] "*If we aren't going to stop a company that is looking inside its subscribers' communications (reading the "packets" they send), blocking that communication when it uses a particular application regardless of whether there is congestion on the network, hiding what it is doing by making consumers think the problem is their own, and lying about it to the public, what would we stop? ....*" And he made it clear in his statement that policy-makers have a duty to "*preserve the vibrant and open character of the Internet*", in order to "*gain the fruits of increased innovation, entrepreneurship, and competition that the Internet has helped deliver*".

The network operators do not like the Comcast order, because it prevents them from doing precisely the kind of "traffic management" which they want to do in Europe – and which they are lobbying for in the European Parliament. It is arguable that the European Internet will take a step backwards, if the current proposals for amending the Telecoms Package (as above) are permitted to remain in their current form.

Why it is an excuse to talk about the "quality of service"

Network operators are advocating "traffic management policies" to safeguard "quality of service". It is arguable however, that in fact, the opposite will be the case. Quality of service is likely to be worse, not better, with differentiated traffic management.

Quality of service in technical terms means that certain specific criteria are measured – latency and contention for example. Latency concerns the volume of traffic and the speed that it travels at. just as on a motorway, when more cars are travelling, the average speed per car slows down, so it is the same on a network. When more people log on, the average speed of each user's connection slows down. It's also the case that if you interfere with the traffic flow, by filtering it off and inspecting each vehicle, before letting it go on its way, the speed experienced by each user will go down too.

There are other factors which affect quality of service[xiv], however, a basic principle is that the more you ask the network to filter, the more complex it gets, and the increased complexity will create more errors.

The network operator's job is to carry the traffic from each user at the speed they expect to get. Traditionally, this means investing in bandwidth. From a public policy perspective, the regulator could be empowered to ask for business case justifications if "traffic management policies" with a function to discriminate, are to be installed as an alternative to investing in bandwidth.

We could think of a scenario where the networks involved in the global structure of the internet would operate with different quality of service criteria. Each network would filter using its own criteria, using different and potentially incompatible manufacturers equipment, turning the Internet as a whole into a more complex whole system , and more likely to experience problems. If different quality of service "tools" were in place, would get a patchwork quilt of networks, where users cannot use applications and services, and cannot access content, because a restriction or a block has been selectively applied by a network operator.

Such a patchwork quilt of networks risks creating a distortion of the internal market – the exact opposite of the objective of the Telecoms Package. And it is a direct threat to the kind of innovation mentioned above, which takes place at the edges or ends of the network, where users can experiment without needing to ask permission.

Discrimination and "preferred" content partners

Network operators are also using the pretext of solving problems of congestion, capacity constraints and avoiding the collapse of the net work in order to justify the demands for a free hand in network management. The telcos argue that the regulator should not intervene in these cases. In reality, their demands have more to do with introducing new business models.

These proposed new business models are about increasing their 'average revenue per user', (the jargon is ARPU) by offering 'differentiated' services[xv] for which they believe they can charge higher subscriptions[xvi]. And it is about managing the cost per Megabit: According to one example from Camiant, a supplier of traffic management technology, the revenue per Megabit decreases as the bandwidth increases – that is, the network operator earns less money per "unit" of bandwidth[xvii] when he offers a faster pipe to the user and therefore cost control - is important[xviii]. Where this is all leading is a concept called 'subscriber personalisation' - a kind of individual Internet where your pre-chosen services and the network operator's preferred partner content are delivered in accordance with a 'policy plan' that you have purchased[xix].

These objectives are clearly exposed in a paper from Telefonica/O2.[xx] It says: "*there are clients that would prefer to have a cheaper "best efforts" package (no minimum QoS) because they only use* *applications that are not sensitive to QoS parameters, for instance users that mainly use the Internet for surfing and email. On the other hand, there are users who are prepared to pay a premium for differing levels of quality depending on the applications they use*." Telefonica/O2 cites videoconferencing, real time multimedia applications (which could include webcasting and television), and remote medical monitoring as applications which need "guaranteed quality levels" because they are sensitive to quality of service. This tells us that Telefonica/O2 is planning to offer these services as separate chargeable services which it will deliver over the 'free' Internet.

Telefonica/O2 goes on to tell us that "*different consumer behaviours have to coexist. This necessarily implicates prioritisation of data streams when congestion in the network is about to deteriorate all user experiences, particularly those who are using QoS sensitive applications*".

Given that those "*QoS sensitive applications*", are Telefonica's own applications, it is therefore evident that Telefonica intends to decide for itself which of its customers applications deserve priority – a discriminatory practice.

From a public policy perspective, this scenario is highly problematic. The concept of 'subscriber personalisation' by default means discrimination and indeed exclusion of large parts of the Internet – it will be no Internet at all. It isn't appropriate to say that some people "only" want email, and basic text web surfing (as Telefonica implies). This implies that people who are new to the Internet (digital divide) like the elderly for example, will be sold a 'basic' service - which would risk increasing the digital divide. It is also becoming evident that the kind of services that will be prioritised are not necessarily those that would be selected as a public policy priority, for example, online gaming. [xxi] Is this scenario an anachronistic solution for digital divide?

Transparency policy or censorship policy?

The network operators claim that traffic management policies will be underpinned by better transparency obligations[xxii], given that any restriction would be highlighted in the final contract with the citizens. In fact, it is not clear how a traffic management policy should be defined and how the user would know whether it is the traffic management policy or some other reason, that is causing content to be blocked, or why he cannot access something.[xxiii]

Citizens do not always know when an operator is filtering, indeed they may have no way of knowing. It is often difficult to tell what is the cause of a slow dowload. It could be the network operator slowing down traffic, or it could be that the user's computer memory is overloaded. That leads to problems for the citizens, who do not know who to blame, and for the network operator, who has to deal with unfair complaints.

Continuing the car analogy, the only way a transparency policy may work is if the regulator oversees it, because so much goes on in the mechanics of the service. The regulator has to take the part of the citizen and look "under the bonnet" to see what the operator is doing, and whether it is really complying. That implies that the operator has to tell the regulator what his policies are, and agree them with the regulator.

In this respect, the transparency obligations in the Universal Services Directive, (Articles 20.1 (b) and 21(3) Common Position and the Parliament's amendments 43 and 49, and in Amendment 107 to the Framework directive are too weak, because they simply say that the network operators have to publish any restrictions to their service. Amendment 107 does appear to allow the regulator to obtain information on the traffic management policies, however, there is no power elsewhere in the directive for the regulator to monitor the operator's activities, and it is not clear whether disclosure of the actual restrictions is required. In theory, an operator could say in the contract small print that he is restricting particular services or applications, and the users would have no recourse for complaint, and so an operator could act as a form of censor.

Furthermore, there is an anomaly, which is particularly evident in the Parliament's revised proposals. According to Amendment 5 to the revised Universal Services directive, or Amendment 107 to the Authorisation directive, users are granted the right to access any content, services and applications - which is a positive guarantee to be enshrined in the new law. However, by the same clause, they may be told by the network operator that they can't access some services. The texts give the operators a *de facto* right to determine what they won't let users access without a clear obligation to disclose to the regulator, thereby undermining the users rights to access. In a democratic society, would people accept it if they were told they could dial any number in the world, except those numbers which the telephone company said they couldn't dial?

What's needed is a genuine guarantee of citizens rights to access content, services and applications, plus a transparency policy, where the operator is made accountable for any decisions to restrict. This can only be done if there is an obligation on the regulators at national and European level, to audit the transparency policies on behalf of the citizen. This was done to a certain extent in the Parliament's first reading text, Article 28 of the Universal Services directive – which was dropped. However it could be reinstated.

The ultimate risk with the Telecoms Package amendments is that they would lead to a situation where "network management" will correspond to filtering management policies. This is a difficult area from a policy perspective. The technology for a very detailed level of automated censorship exists, and, although it has not yet been proven to work on an Internet access network, the history of technological development tells us that it will work one day. One of the companies which makes the traffic management systems, Allot, sells what it calls a 'copyright sensor'. This piece of equipment claims to take redirected peer-to-peer (P2P) traffic from the Internet, analyse it to identify copyrighted content, and "alert the network gateway upon violation"[xxiv]. Audible Magic, another equipment-maker, claims to have a database of 6 million sound recordings, and sells its technology to network operators for copyright filtering – although the Audible Magic equipment has been shown not to work in the case of the Belgian ISP Scarlet, which demonstrates how problematic this area is. Allot technology was also rejected by Scarlet[xxv]. Such filtering is expensive, and in the Scarlet case, would have put 0.5Euro per month onto the bill of every subscriber.

From a policy perspective, when putting in place legislation to last for several years, it is important to consider the regulatory implications of such a censorhip scenario. How is rationally possible to draw a line between prioritizing traffic, choosing which citizens to give a certain type of services, and controlling the citizens? The amendments to the Telecoms Package, in their current form, fail to deal with such a scenario. Instead, they imply that filtering may be carried out, with only a minimum level of protection for the end-user, and the Article 29 Working Party has warned that Article 6(7) [formerly Article 6.6(a)] of the e-Privacy directive could open the way for wide-scale deployment of deep packet inspection.

A regulatory policy to deal with "traffic management"

Given the level of uncertainty of how "traffic management" systems will impact on users experience, and the surreptitious and automated control that it places in the hands of the network operators and ISPs, it makes sense to ensure that there are appropriate powers for regulators to oversee and intervene.

Some argue that competition law will take care of discriminatory practices by network operators. However, as Valcke et al [xxvi] point out, competition law prohibits the abuse of dominant positions, and targets distortions of competition which results from agreements or collusion. The Single Market Power regime in the Framework directive deals with market dominance, and the Access directive, Article 5 (referred to in the Council text, Recital 14) in the existing law, ensures the end to end interconnectivityof networks. These remedies- especially the Article 5 - are helpful, but at the same time they are limited in their application (if at all) to citizens rights and certain potential problems that could be createdd by " traffic management systems."

The European Data Protection Supervisor has recently advised that Article 5 of the ePrivacy directive, would apply where "traffic management policies" entail interception and surveillance, and the user's consent would be required and it is noted that this has been reinstated into the Parliament's Second Reading text[xxvii]. It is also argued that consumer protection law will take care of the consumer's rights. However, it is the job of the Universal Services directive to take care of consumer rights in respect of telecoms networks and this amendment – and it is ironic that the amendment that may erode users' rights is in that same directive.

Similarly, the reinsertion of both Amendments 138 and 166 from the 24 September text, into the Parliament's Second Reading texts, is helpful. . These amendments put in place a framework safeguarding users against potential abuses. Amendment 138 says that a court order must be obtained before a restriction may be placed on the fundamental rights and freedoms of users. The intent was to deal with graduated response and sanctions such as termination of internet access. Amendment 166 says that any restriction on users rights to access content, applications and services must be dissuasive, effective and proportionate. The safeguards implied in these amendments could act as a counterweight to discrimination by "traffic management" but only if the regulator has the power to do anything.

Therefore, from a public policy perspective, the important element is regulation. The problem is that the regulator's toolbox is almost empty of tools to deal with these new situations that will arise. The regulator - both national NRAs and the new EU regulatory body – will need to have the power to get involved in cases where "traffic management" is used to discriminate in favour of new services, or where it is used to support 'reasonable usage restrictions, price differentiation and other competitive practices'. As the Telecoms Package text currently reads, the only tool they have is quality of service specification, which will be inadequate if they need to intervene as the FCC successfullly did. It's important to understand that the FCC intervention in the Comcast case, was not about discrimination or anti-competitive behaviour against another network operator. It followed a complaint from Vuze, which operates television-like services using peer-to-peer technology *over the top* of the Internet, concerning Comcast's blocking of peer-to-peer traffic. The case concerned unfair discrimination against particular content and applications. Comcast, which also runs television services, was deemed to be anti-competitively blocking Vuze services, and to be discriminating against peer-to-peer users in general.

In respect of public policy decisions, the Internet is not not just about markets and consumption. The Internet is about citizens, and the issues for policy-makers concern as much the citizens' fundamental rights to access and distribute information, to free speech and to privacy, as they concern rights to buy or sell. Millions of European citizens have helped to build the WWW, and they will be concerned to defend their stake in it. If a similar case to Comcast should occur in Europe, the national regulators (NRAs) , as well as the new pan-European body (BERT or GERT), need to have similar powers to the FCC to intervene. Under the current construction of the Telecoms Package, this is doubtful. Indeed, it seems more likely that they would be held back and constrained from doing anything. It will be important that the network operators can be held accountable for their 'traffic management policies' in a two-way transparency policy, and that the new pan-European regulator, as well as the NRAs, should have real power to address a Comcast-type situation. And most of all, European public policy needs to protect all layers of the Internet, by guaranteeing its neutrality.

The authors, Monica Horten and Benedetta Brevini, are PhD researchers in EU media and communications policy at the University of Westminster.

[i] Article numbers refer to the Council Common Position of 9 February, unless otherwise specified. Amendment numbers refer to the European Parliament revised versions of the 23 February 2009, unless otherwise specified.

[ii] Article numbers refer to the Council Common Position of 9 February, unless otherwise specified.

[iii] Lawrence Lessig & Robert W. McChesney (8 June 2006). "No Tolls on The Internet". *Columns*. Washington Post. http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/AR2006060702108.html.

[iv] This is enshrined in EU law as the 'mere conduit' principle , Ecommerce directive, Article 12.

[v] Cooper, M (2004) "Maching the network connection.Using Network Theory To Explain The Link Between Open Digital Platforms And Innovation" in Cooper, M *Open Architecture as communications policy.Preserving internet freedom in the broadband era,* Center for Internet and Society, Stanford Law School

[vi] Viviane Reding, Internet of the future: Europe must be a key player, speech given at the Future of the Internet initiative of the Lisbon Council, Brussels, 2 February 2009

[vii] Lawrence Lessig, (2001) The Future of Ideas , p39

[viii] Milton Mueller, (2002) Ruling the Root, Internet governance and the taming of cyberspace, p101

[ix] Valcke et al, (2008) Network Neutrality, Legal answers from an EU perspective p4

[x] PRESS STATEMENT OF CHAIRMAN KEVIN J. MARTIN Re: Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications; Broadband Industry Practices, WC Docket No. 07-52

[xi] Formerly Article 33(2a) of the Universal Services Directive (Harbour report).

[xii] Viviane Reding, 2 February 2009, ibid

[xiii] ibid, PRESS STATEMENT OF CHAIRMAN KEVIN J. MARTIN

[xiv] For example, the location of the filtering equipment in the network – core, access or backhaul – will impact on QoS; as will the speed and processing power of the filtering equipment itself.

[xv] Digital Britain, (2009) Section 2, p9

[xvi] The telcos perceive that content companies and specifically those selling subscription TV services, make a higher revenue per user, and that is the extra revenue that they are chasing.

[xvii] It isn't strictly correct to speak about a "unit" of bandwidth, but this is the simplest way to understand it.

[xviii] Light Reading webinar, Next-Generation Broadband Packages: The Role of Policy Control, 27 January 2009,. From www.camiant.com "Camiant's suite of policy control platforms simultaneously manage network utilization and guarantee assured delivery of multimedia applications over broadband networks."

[xix] Light Reading webinar, 27 January 2009, ibid

[xx] Telefonica/O2 Network Fairness, a consumer focussed approach (16.10. 2008).

[xxi] Netconfidence coalition, Ensuring Network Stability and consumer confidence in comepetitive markets, p2

[xxii] Netconfidence coalition, Ensuring Network Stability and consumer confidence in comepetitive markets, p1

[xxiii] ibid Valcke, et al , p 26

[xxiv] Light Reading webinar, Making the most of DPI, 19 November 2008

[xxv] Court documents: Sabam v Scarlet, Tribunal of the First Instance, Brussels.

[xxvi] ibid Valcke et al, Section 4.2

[xxvii] EDPS comments on some issues is the review of Directive 2002/22/EC (Universal Services) pp5-6