Briefing Paper - Deep packet inspection, copyright and the Telecoms Package - DRAFT
Monica Horten
University of Westminster, Communications and Media Research Institute
PhD Research – The Political Battle for Online Content in the European Union
26 August 2008

Deep packet inspection, copyright and the Telecoms Package

How Europe's Internet could be restricted on behalf of industrial interests

The Telecoms Package has amendments which permit ISPs to degrade and restrict content provided it is in the small print of the contract with the user. The impact is to reduce the liability of Internet Service Providers for degrading and restricting services, applications and content. The words 'degrading' and 'restricting'   have special meanings in the telecommunications world. They mean 'slow down' and 'block'. Thus, these amendments are really talking about the slowing down of user's connections and the blocking of access to websites and applications.

The technology which the ISPs will use to do this is called deep packet inspection. This means that the data on the network is literally opened up and checked for what it contains. The ISP makes a decision about where to forward it, based on the contents. Deep packet inspection can be used by the ISP for managing the network in a benign way, but it also is a powerful technological tool for censorship. It is in place on all of Europe's telecommunications networks.

In China, deep packet inspection is used for censoring the Internet. The difference between Europe and China is that we have laws forbidding censorship. The E-commerce Directive says that ISPs must not monitor content.

The copyright industries have been lobbying for deep packet inspection to be used to monitor for copyright infringement. Specifically, they want peer-to-peer applications, websites and services blocked. The only way to do this is to use deep packet inspection. In some cases, this means intercepting individual downloads. There are also demands to filter traffic against a database of 6 million songs. In these instances, deep packet inspection results in degradation and restriction of services – and thus the amendments to the Telecoms Package take on a real-life significance.

In respect of the Telecoms Package, we are on the verge of a step-change in telecommunications service provision, with serious implications for citizens privacy, business innovation and censorship, but we are legislating to support last-century business models. We are putting in place a law which sanctions the interception of people's private communications and permits content to be blocked on behalf of industrial interests, who will supply the blocking criteria. People will be arbitrarily blocked from using the lawful applications of their choice.

Europe's policy-makers should take positive steps to

- **protect the diversity of cultural content and democratic discourse on the Internet, ensuring that users have access to a multiplicity of sources**
- **protect Internet users from interference – interception, redirection or blocking - by governments or corporations.**

Briefing Paper - Deep packet inspection, copyright and the Telecoms Package - DRAFT

Monica Horten
University of Westminster, Communications and Media Research Institute

PhD Research – The Political Battle for Online Content in the European Union
26 August 2008

Deep packet inspection, copyright and the Telecoms Package

How Europe's Internet could be restricted on behalf of industrial interests

Europe is installing a telecoms infrastructure capable of censorship on an Orwellian scale, that has until recently only been dreamed of by the large corporations who would control our lives. The all-seeing electronic Panopticon is buried in the equipment that sends our data around the Internet[i]. The copyright industries know this. The rest of us are in a lull from which we will only be awoken when we find our keyboards silent and our mice gagged and all we can do on what was once the Internet is watch television programmes produced by the Hollywood moguls and listen to bubblegum muzak from the big four.

An exaggeration? Attention-getter? Possibly. But listen more closely. There is something happening out there which policy-makers and citizens need to become aware of. It's a new technology on the up and up, which has a tremendously powerful capability to look into what we do on the Internet and to act as a gatekeeper, security man and policeman.

It is especially important in the context of the Telecoms Package and the discussions about the copyright amendments. In the haste of MEPs to backtrack on the specific references to copyright, which make the law more difficult for anyone but a lawyer, we are in danger of overlooking the fact that copyright enforcement can take many forms.

Just imagine your broadband provider was able to check every download you make against a database of 6 million songs[ii]. It could stop you or let you carry on, and it would decide what to do against a set of IFPI-defined criteria. This is not a figment of my imagination. The database has been developed by a company called Audible Magic, which is selling its wares to Internet companies all around Europe. Last year, it managed (or its lawyers did) to convince a Belgian court that an ISP could use the database to check for copyright infringements by its users.[iii]

Alternatively, consider that your Internet service provider was able to look into every packet of data that you transmit – just like an electronic post office, it would open the envelope and look inside, and it would decide what to do with it on the basis of what it found in the contents. According to a politically-determined criteria, your packet either carries on to where it is going or you get redirected to a page like this: 'POLICE NOTICE. Access denied in execution of a court injunction'[iv]. Chinese people will tell you they are used to this kind notice – or even just a blank screen. But in Europe?

Courts in Italy and Denmark[v] have ordered the blocking of peer-to-peer websites by ISPs. The reason for picking on peer-to-peer websites is the result of extensive lobbying by the music industry, which has cited the peer-to-peer demon[vi]in every political venue where it can get a hearing, and is arguably politically-motivated. In order to block access to the site, Internet service providers have to look into the packets of data and they have to send an individual signal to every user they are being asked to block. But, in many cases, exactly the same content is available on other websites, and is freely accessible.

What I have just described are two methods of copyright enforcement, which don't mention the word 'copyright'. And it is precisely these kinds of scenarios, and this new technology – known as deep packet inspection – which we need to think about when considering the Telecoms Package amendments. Deep packet inspection is an advanced network technology that has many positive uses for the Internet providers. However, its misuse is what policy-makers need to concern themselves with.

Deep packet inspection explained

Deep packet inspection technology, in simple terms, means that the individual pieces of data travelling on the Internet are looked into to see what they contain. Deep packet inspection has been around for a number of years. I am reliably informed that it was possible over 10 years ago, and that a trial was conducted within a major equipment vendor, looking into the traffic of an individual on the network. At that time however, it wasn't scalable, that is, it wasn't feasible or cost-effective to set it up on a large scale network to look at multiple users. Things change. It is now.

To understand it better, you need to know a bit more about the Internet and how it works. Data on the Internet travels in 'packets' – that is, the stream of bits and bytes that goes out from your computer, is quite literally, split up in separate pieces, and each piece is put into a 'packet' with the address of the website that you want to visit, or the server that you are transmitting to. The address on the outside of the packet is normally known as the packet header.

Your packets don't travel in one continuous stream. Instead, they are sent between servers on the network, based on the address on the outside of the packet. Just like a post office or courier will send your real-world packets, so the Internet sends your data packets. The packets from the same file may travel via different routes on the network and when the packets reach their destination, they are put back together again into a single file, just like an electronic Humpty Dumpty.

For simple transmission purposes, the Internet service provider only knows the information that is in the packet header – address, time stamp and other data known as communications data. With deep packet inspection, the Internet provider intercepts the traffic flow, and looks inside the packets to see what you are doing. Having looked, it will check against its own files, to find out what to do with your data. This is an automated process happening at massive speeds – the latest equipment can do it at a phenomenal 10 Gbits per second[vii].

Early systems just monitored, looking for problems in the traffic flow and for security breaches. They were passive, and limited in use, being placed only at a few specific points on the network. For us as consumers and citizens, they were most probably performing a positive function.

But as we've already noted, things have changed. Today's systems are no longer limited to specific control points on the network - they are designed to go at the heart of the network, and at the outer edges. What this means is that the provider has the ability to interfere with the traffic flow at different levels in the network. It can do it on an aggregate basis in the interior of the network – like a highways agency managing motorway traffic. But it's the edge equipment that is really interesting, because it is this equipment that enables the provider to look more deeply at the traffic from you and me, and all individuals[viii].

And the providers can not only intercept the packet to look inside, they can actively interfere with its transmission. They can stop it completely from travelling, preventing you from viewing the website you were wanting to look at, or from downloading a file you were trying to get. In relation to the Telecoms Package, it is significant that they can *impose restrictions on content, applications and services*[ix]. They can redirect your traffic to a web page owned by someone quite different from the website you wanted – in the Italian example I gave above, the police notice put up on the orders of the Italian court, redirected to a page on a server owned by the IFPI.[x]

And today's systems have advanced a long way from simple traffic flow and security monitoring. The deep packet inspection systems take their orders from large database files, which are programmed with a series of rules in the form 'if you find this, then do that'. The sales pitch from the manufacturers for the systems suggests a number of purposes for which the rules can be written. These purposes include advertising, managing subscriptions, prioritising different types of traffic, and specifically, controlling and blocking peer-to-peer applications and copyright infringing content[xi]. For example, Nortel Networks claims: *Peer-to-Peer file sharing traffic on a network can be identified and subsequently restricted to a specific amount of bandwidth on a per-user or aggregate basis*[xii] In plain English, this means they can block peer-to-peer traffic as a group, which they might do on the backbone or main trunk arterials of the network. And they can block an individual connection to a known user.

It is not one hundred per cent sure that it all works. In spite of extravagant claims by the manufacturers and the massive 10 Gigabits per second throughput speeds, the Internet service providers say that deep packet inspection for the purposes of checking and redirecting content doesn't work so well. The problem is that it slows down the entire network. And significantly, in relation to the Telecoms Package, the technical term is *degradation of service*. All Internet users are inconvenienced, for the sake of copyright infringement checks, for example.

In the Belgian case[xiii], the IFPI-populated Audible Magic database is used to supply the criteria for interference is another. In this instance, the court asked for tests to be run, and the case is *sub judice* pending the outcome. However, the technology is improving all the time, and whatever the test result should be, the key question here for policy-makers is whether IFPI, or any third-party organisation, should be able to demand the right to determine what happens to our web traffic.

The European deep packet infrastructure

Deep packet inspection systems are being installed around Europe, and they give the Internet providers tremendous power over how we as citizens, communicate.

The leading manufacturer is Cisco, which offers deep packet inspection on its major product lines. Cisco is also the company whose products have been used to build the great firewall of China – the ability of the Chinese government to use this technology to censor websites is well-known, and was highlighted again recently in the press coverage of the Beijing Olympics. Cisco's long standing competitor is Nortel Networks, which also offers deep packet inspection in its products. Thirdly, there is an up-and –coming company from Canada called Sandvine, whose products are installed a number of north American networks and in two cases, the application of the deep packet inspection technology in those networks has been the subject of litigation[xiv].

All of Europe's major telcos have networks based on Cisco equipment – Deutsche Telekom, Telecom Italia, Telefonica, BT and France's Orange (formerly France Telecom) and Neuf Telecom - are among them. The equipment they have installed has deep packet capability, although it may be an optional function on some routers, and so it may or may not be actually activated yet. [xv] BT has recently placed a contract with Cisco for the latest equipment just released in March 2008, which has built-in deep packet inspection.[xvi] In the new EU member states, the infrastructure is also going in, for example, Max Telecom in Bulgaria.

And it's not just the fixed wire telcos, it's the mobile companies too. Cisco's product brochures highlight deep packet inspection and content filtering within its mobile network product line:

"*When users request content, the request is intercepted and compared against a filtering database for that particular user... Requests for allowed content are fulfilled as usual, and requests for disallowed content are blocked or redirected to a server that indicates the request cannot be fulfilled*."[xvii]

Vodafone has Cisco-based networks. Sandvine has sold equipment to the UK's Carphone Warehouse which will give it *granular visibility into subscribers' usage patterns*'[xviii]. In plain English, that means it can see what you and I are doing. Sandvine has also sold to Liwest Kabelmedien in Austria and boasts of having sold to other European telcos which it will not name.

Deep packet inspection and restriction of content

What this means is that Europe has the equipment to censor on a similar scale to the Chinese. The nature of the censorship is determined by the database file that tells the deep packet inspection system what to do. It doesn't really make any difference if the file is supplied by the IFPI, or the government, it amounts to the same thing.

Deep packet inspection is the main technical tool that would be used today in circumstances where content is to be censored or blocked – and for copyright enforcement. Other tools include IP address, domain or URL blocking and DNS poisoning, and collectively, all of these techniques are referred to as filtering[xix].

The difference between Europe and China is that our law doesn't permit that kind of abuse. Not yet. The concern is that an apparently harmless alteration to the law, within the Telecoms Package, pushed through in a hurry, will permit it to happen. Once the law is changed, it will be difficult to reverse.

The E-commerce Directive establishes the principle that Internet providers are 'mere conduits' - they carry the traffic, but they do not know or care what it contains[xx]. The E-commerce directive also forbids governments from asking Internet service providers to monitor traffic and to look into their customers' content. The door is firmly closed to censorship of content – for any purpose – on the Internet. People who have a grievance with material that is published, have the usual legal routes open to them, such as court injunctions.

The problem with the Telecoms Package is that it pushes that dangerous door open. It doesn't say directly that Internet providers can monitor. It can't do that, because the E-commerce directive stands in the way. It does, however, reduce the liability of the provider for degrading traffic and restricting content. It says that Internet providers must state the nature of any restrictions in the users' contract (ITRE Amendment 121, IMCO Amendments 11, 12, 13,14, 62, 75, 81). Also built in to the Telecoms Package is a requirement that Internet Service Providers should be asked to 'cooperate' with rights holders, where cooperation in this context is frequently defined as including filtering and blocking of content[xxi], and the clauses on restriction of content should be read in this light. Network management purposes are expressly excluded from this. Therefore, there must be some other purpose for which the Internet provider might wish to *degrade traffic* and *restrict access to content, applications and services*.

Here is the actual text: '*users should in any case be fully informed of any restrictions and / or limitations imposed on the use of electronic communications services...Such information should...specify either the type of content, application or service concerned, or individual applications or services or both*[xxii]'. It seems clear from the way the text is written that there is an intention to restrict access to specific applications, content and services. The tool for doing it is deep packet inspection.

Deep packet inspection and industrial interests

In the wider context, we know that the music and the entertainment industries are pushing for the Internet service providers to use deep packet inspection to support their claims of copyright infringement. One method they are demanding at the moment, is that ISPs should use deep packet inspection techniques to block access to peer-to-peer file sharing networks, and even block all peer-to-peer traffic. Their demand is based on their claim that a significant amount of downloads where are allegedly infringing copyright come from such peer-to-peer file sharing websites.

Litigation is an ancillary tool to their political lobbying. There are several European law suits which have been pressed either by IFPI or by other organisations representing the music industry. The target is to close down peer-to-peer websites, either by suing them directly, or by suing the Internet providers. The Belgian case was filed by the collecting society, Sabam, against a small Internet service provider called Scarlet, and it specifically targeted peer-to-peer content. The merits of blocking, and how to block, peer-to-peer were argued over in the courtroom. The other two law suits in Denmark and Italy (mentioned above), concern requests to the provider to block a specific peer-to-peer website, called The Pirate Bay. The Italian case was filed by the local IFPI associate and anti-piracy group, FPM, and the Danish case by IFPI Denmark. The only way they can block the site is to use deep packet inspection. This is due to the nature of peer-to-peer traffic – the other filtering techniques like URL blocking will not work for these sites[xxiii].

There is also a case against the Pirate Bay in Sweden, which has been filed by the Swedish public prosecutor, following IFPI pressure on the Swedish government. The Motion Picture Association, representing the powerful Hollywood lobby, has followed behind with a further claim for damages from The Pirate Bay.

IFPI's Irish member is suing Eircom, the Irish telecoms provider. The case states that Eircom has refused to install the Audible Magic technology, following a request from the Irish Recorded Music Association (IRMA).[xxiv] In the UK, some Internet providers are already using deep packet inspection to slow down – or "throttle" - peer-to-peer traffic. In France, the Internet providers have been asked to test deep packet inspection for copyright enforcement, with a view to a full scale compulsory implementation.

Talking to people from the music industry, one hears an oft-repeated whinge along the lines of 'they (the Internet providers) can do it when they need it for their business, but when it comes to us, they say they can't do it?' The written communications to the European Commission from IFPI call for by Internet providers to support copyright enforcement by *blocking access to specific protocols or infringing sites*[xxv]. The Motion Picture Association calls for "*the take-up of technological tools*" and with reference to the Sabam vs Scarlet case, it demands content filtering solutions using film databases to provide the criteria for blocking or allowing user access. It is part of their drive for "*co-operation*". [xxvi]

Who makes the deep packet decisions?

It is arguable that the Internet industry has been right to refuse the IFPI and MPA requests. It is likely that they know better than anyone what a powerful technology they literally hold at their fingertips. With a few keystrokes, they could wipe someone's presence off the web. And it is reasonable that they are reluctant to take on the responsibilities and liabilities of implementing what is effectively a form of censorship on behalf of another industry which is dictating the criteria – criteria that are set according to a law which contains complex exceptions to the general rule of copyright ownership and not harmonised across the 27 EU member states. The experts maintain that computer code alone cannot distinguish between infringing and non-infringing content.[xxvii]

It is worrying then, that deep packet inspection systems are being actively touted to the Internet providers by the manufacturers for 'policy management'. Audible Magic's products will '*automatically filter P2P and enforce your network-use policies*'. One has to ask 'whose policy' are they managing and what is it? At a seminar I attended[xxviii], a representative of Audible Magic said that the 'network manager' made the decisions on the content filtering criteria. The product literature from other vendors takes a similar view.

What is acceptable to the European citizen?

As policy-makers, we need to understand the full implications of this powerful technology, and do our best to legislate so that it is used positively for the benefit of European citizens. Not rushed through, to meet a flawed set of deadlines.

Given our understanding of the context, where deep packet inspection is intended for use in blocking peer-to-peer Internet traffic and websites, there are three issues. Most importantly, opening the data packets and looking inside an individual user's traffic counts as interception of a private communication. This is illegal under European privacy law.

Universally blocking peer-to-peer traffic to enforce copyright - as the music industry is demanding - is an arbitrary method of blocking and it discriminates against those users who use it for other purposes (ie those who are not downloading copyrighted music or film or acting in breach of copyright law). It's rather like stopping all white vans on the motorway because they generally are driven by young men who might be transporting something illegal.

There are many users of peer-to-peer who are not infringing copyright. It is well known that musicians use peer-to-peer to promote their work. The British band Radiohead, for example, released its new album for free on the web, asking fans for a voluntary donation. This example is widely cited and the usual story we hear it that the band made no money. However, according to a report just released by the UK artists collecting society, the MCPS-PRS[xxix], that is not the full story. There were 2.3 million downloads of the album on pirate websites. If we take the classic music industry story, we would believe that this represents 2.3 million lost album sales and therefore the pirates must by pursued and penalised. But three months' later, in January 2008, the album on CD sold so well it went to number one in the UK and the US, and fans are paying £50 a ticket for Radiohead concerts. The pirate downloads therefore represent not lost sales, but a vital promotional tool, without which the band might have made no money at all!

A recent decision by the US Federal Communications Commission supports this view that peer-to-peer blocking is arbitrary and discriminatory. The case concerned a complaint against the Internet provider Comcast, for secretly degrading peer-to-peer applications[xxx]. The FCC determined that Comcast had blocked and delayed customers simply because they were using a disfavoured application, and that Comcast's claims that it was done for network management purposes were not justified. The FCC went on to say that blocking of peer-to-peer in these circumstances is a arbitrary block of a particular application. and it ordered Comcast to cease the practice, saying that all customers have a right to unfettered access to the Internet.

"*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?*" said commissioner Martin in his press statement.

Blocking peer-to-peer web traffic is also potentially an anti-competitive move. This of course, depends on the Internet provider. But take a provider such as Sky, or Deutsche Telekom, which both offer paid for television services. Might it not be in their commercial interest to block peer-to-peer traffic? There are a number of new and innovative (and European) services which are using peer-to-peer technologies to deliver new-style television such as Joost and Vuze. This is the television of the future – and competition for the incumbents.

I am not here to cast blame where it does not lie, but I do feel it is important for policy-makers to understand the potential developments in the industry, before casting a policy vote.

Another interesting conundrum for policy-makers is who should take the decision as to which peer-to-peer traffic should be blocked and which should be allowed. Because there are different types of peer-to-peer traffic. The one that the music and film industries don't like is called Bit Torrent. But there's another one, called Kontiki, that is used by the BBC iPlayer, and indeed, by Sky. We have to ask ourselves whether the decision to block either Bit Torrent or Kontiki should be left to a network manager or whether it should be taken at a policy level for the benefit of the whole of society.

There is an over-riding issue here about what kind of Internet we want in Europe. Not just whether we want to allow censorship by the music or any other industry, utilising the powerful deep packet inspection technologies, but also whether we want to go back to the days when our entertainment and news was under the total control of one or two organisations. Lawrence Lessig, law professor at Stanford University and long-time campaigner for a free Internet, says that the current battle for the Internet rages around two alternative futures: the traditional television model, where the network owners get to choose what content we can watch; or the traditional telephony model where the user alone chooses with whom he connects and what he says, and the network operator has no right to interfere.[xxxi]. It is arguable that anti-competitive blocking of peer-to-peer traffic, as demanded by the music industry, is the first step towards controlling the available content, and funnelling it all through the channels of the commercial providers.

Europe's policy-makers must deal with deep packet censorship

Given the immense power of deep packet inspection technology to censor as well as to provide, Europe's policy-makers need to pay more attention to it.

In the specific context of the Telecoms Package, it strikes me that this set of directives is supposed to provide the framework for telecommunications law for the foreseeable future. And yet, we are incorporating without proper public debate, changes which will open the door to the Orwellian scenario I described at the beginning. We are putting in place a law which sanctions the interception of people's private communications and permits content to be blocked on behalf of the music and entertainment industries. These industrial interests will supply the databases with the blocking criteria. People will be blocked from using the lawful applications of their choice.

We are on the verge of a step-change in telecommunications service provision, with serious implications for citizens privacy, business innovation and censorship, but we are legislating to support last-century business models. This is a legal review for yesterday, and it ignores the implications for tomorrow.

In the context of the Telecoms Package, Europe's policy-makers should seek to:

- Protect users' access to a diversity and multiplicity of sources of cultural content and democratic discourse
- Protect the principle of 'mere conduit' and the telephony model for the Internet
- Protect Internet users from interference - interception, redirection, blocking - by private corporations or governments

You are free to use the information in this paper, provided you attribute it to the author. To discuss the issues raised in this paper, please contact the author. Monica Horten is carrying out PhD research in European communications policy at the University of Westminster. Tel: +44 (0) 1628 672155 Website: www.iptegrity.com

[i] For example, all Cisco 6500 switches, installed by several European ISPs including Deutsche Telekom and Telekom Italia, have a deep packet inspection technology capability.

[ii] Audible Magic http://www.audiblemagic.com/products-services/registration/

[iii] Sabam v Scarlet District Court of Brussels, No. 04/8975/A, Decision of 29 June 2007 Translated by Fran Mady, Julien Bourrouilhou, and Justin Hughes, Cardozo arts & entertainment journal, Caelj Translation Series #001

[iv] Guardia di Finanza, Nucleo di Polizia Tributaria Bergamo, Available at: http://217.144.82.26/pb/. Server belongs to Reactive Networks which hosts IFPI site pro-music.org

[v] Tele2 case in Denmark, February 2008; court order by judge in Bergamo, northern Italy, 8 August 2008

[vi] William Patry, legal counsel for Google, Intellectual Property Quarterly (2008) Metaphors and moral panics in copyright: the Stephen Stewart memorial lecture, November 13, 2007

[vii] Dave Voraus, RCR Wireless News, 9 June 2008

[viii] Based on product brochures from Sandvine, Nortel, Cisco and Audible Magic.

[ix] IMCO Amendment 11 and Amendment 75 (Recital 14 , and Article 21, par 4).

[x] ibid iv. Guardia di Finanza. Published in a report on TorrentFreak, and verified by myself using reverse IP and Whois lookups.

[xi] ibid Audible Magic. Nortel, Cisco product brochures available online.

[xii] Nortel Networks, *Traffic management product bulletin: What is policy-based traffic management?*

[xiii] ibid Sabam v Scarlet

[xiv] Comcast case adjudicated by the FCC; and the Bell Canada case, which is ongoing at the time of writing.

[xv] For example, the Cisco 7600 routers require an upgrade installing a new line card such as the CSG2 – Content Services Gateway 2nd Generation - that has been available since March 2007.

[xvi] Antony Savvas, Computer Weekly, BT to deploy cost-saving Cisco router as part of network contracts. The ASR1000 Series routers are based around the Quantum flow processor, which has DPI as a function. Other sources are Cisco press releases and published information. Cisco 65xx series switches, 7600 routers, 10000 and 12000 series router products feature deep packet inspection.

[xvii] Cisco White Paper (2007) Mobile Content Filtering and Control: Why it is Needed, How it Works. Discusses the Cisco mobile Service Exchange Framework (mSEF).

[xviii] Sandvine press release 8 August 2007. Sandvine will demonstrate its products at the BBWF Europe, booth 346 held in Brussels, September 30 - October 2, 2008.

[xix] See my website www.iptegrity.com 'What is filtering?'

[xx] See my previous paper: The 'Telecoms Package' (Paquet Telecom) and the copyright amendments – the legal framework for a censored Internet

[xxi] See my previous paper for an analysis for "co-operation" in this context : The Telecoms Package and '3 strikes' – voluntary cooperation to restrict downloads

[xxii] IMCO report, Recital 14

[xxiii] The actual technique used is TCP packet reset. Ref. Malcolm Hutty, Linx, presentation at the ISP Future Content Models and Enforcement Strategies, 7-8 July, London

[xxiv] The Irish Independent http://www.independent.ie/national-news/eircom-may-face-music-in-illegal-files-row-1313154.html

[xxv] IFPIand MPA submissions to European Commission Consultation for Creative Content Online, February 2008.

[xxvi] See my previous paper for an analysis for "co-operation" in this context : The Telecoms Package and '3 strikes' – voluntary cooperation to restrict downloads

[xxvii] Viacom International Inc v YouTube Inc and Google Inc, Opinion and Order, 1 July 2008, p5

[xxviii] ISP Future Content Models and Enforcement Strategies, 7-8 July, London.

[xxix] MCPS-PRS Economic Insight, Issue 10 29.07.2008. *In Rainbows On Torrents.* Available at: www.mcps-prs-alliance.co.uk

[xxx] 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,

[xxxi] Lawrence Lessig video blog http://lessig.org/blog/2008/08/me_on_mccain_on_technology.html