All-Party Parliamentary Group on Communications

Inquiry into the role for Government over Internet traffic

Response from:

Professor Steven Barnett
Dr Maria Michalis (*contact person*, email: m.michalis@westminster.ac.uk)
Monica Horten, MA DipM
Benedetta Brevini, LLM MSc

CAMRI (Communication and Media Research Institute)[1]
University of Westminster
Harrow Campus
Watford Road, Northwick Park
Harrow HA1 3TP
Tel: 020 7911 5000, ext 4549
Fax:020 7911 5942

22 May 2009

[1]CAMRI is a global centre for media and social change. It provides expertise in media policy and economics, media history, and media audiences. In the 2008 Research Assessment Exercise it was rated as the best media and communication research centre in the UK. For more information, access http://www.wmin.ac.uk/camri

We welcome the opportunity to respond to the Inquiry of the All-Party Parliamentary Group on Communications and we set out herewith our position on questions 1 and 5.

Question 1

This question falls into two parts.

Can we distinguish circumstances when ISPs should be forced to act to deal with some type of bad traffic?

In relation to the content they carry, ISPs have a 'mere conduit' status. This is enshrined in the EU E-commerce Directive that has been ratified in the UK by the Electronic Communication Regulations 2002 and clearly specifies that ISPs are carriers not content providers.[1] Their role is to transmit data, but not to deal with the content of the data.

It is appropriate to define what is meant by "bad traffic". In the context of this question, we understand it to mean data carried over the Internet which falls into the following categories:

Illegal content: this refers to ISP responsibilities under criminal law, and specifically to child pornography. ISPs are obligated to implement limited block list from the Internet Watch Foundation (IWF).

Harmful content: such as spam, viruses, and malware, which may damage the integrity and security of the networks and the devices attached to them.

Unlawful content: that is content which breaches a right or creates a tort, e.g. copyright infringement, and defamation.[2]

Undesirable content: which is distasteful or offensive to some, but is not illegal, such as adult pornography.

The law as it stands today, permits ISPs to deal directly with illegal and harmful content. In respect of unlawful content, there are established legal remedies under the relevant law on copyright and defamation, in cases where Internet content is deemed to infringe a right.[3] In respect of undesirable content, it is the responsibility of the end-user or consumer to take action and set up filtering software on their own computer if they wish.

When should we insist that ISPs should not be forced into dealing with a problem, and that the solution must be found elsewhere

Our answer is based on the assumption that the "problem" relates to unlawful content, and undesirable content. And that the "problem" with unlawful content refers to copyright and peer-to-peer downloading or file-sharing, and user generated content. The real "problem" is that the Internet has altered the scale of the activity of copying and distributing copyrighted content from one which was mostly commercial in nature, carried out by a few individuals, to one which may be carried out by any otherwise respectable individual, using a home computer. Thus there is a large number of people, carrying out small-scale copyright infringements – so-called piracy. The underlying issue concerns the economics of content distribution, which ultimately feeds back into content production. This whole issue is complex and is widely debated, and the views on it are highly polarised. The creative industries call for more stringent enforcement. The Internet industries argue it is a question of changing the business model. It is our view that policy-makers should seek to understand the underlying business issues in order to help find alternative ways to protect creativity. It is also our view that the "problem" should not be tackled by the infringement of the individual's privacy rights, and we highlight that certain methods proposed for addressing this "problem" raise civil liberties issues.

Unlawful content: The existing copyright law allows for a '*notice and take down'* procedure, which permits rights holders to ask website owners (including websites such as *YouTube*) to remove copyrighted content. The issue here is that the criteria for asserting the rights of the rights holders versus the rights of users are complex. Therefore, owners of websites and user-generated content sites tend to remove content on the basis of a claim, without being able to establish conclusively whether the claim is justified. Notice and take-down procedures only concern ISPs where they provide web hosting services.

A method that has been proposed for dealing with copyright infringements is the *graduated response*, also known as "*3 strikes and you are out"*. Anyone alleged to have downloaded a copyrighted file, may receive a series of warnings and be sanctioned by cutting off their Internet access. This method has privacy implications because it involves the use of personal data held by the ISPs, and it involves online surveillance on users' online activities in order to identify the alleged infringing files. Depending on how it is implemented, there may be other issues related to the imposition of sanctions. For example, cutting of Internet subscriptions is problematic where the subscriber may or may not be the same person as the alleged infringer. France has recently introduced a law on graduated response, which has been opposed by civil liberties groups and opposition parties.[4] UK proposals, under the Digital Britain Rights Agency consultation, to send notifications to users and potentially to resort to technical measures to sanction users, would fall into the same category from a policy perspective.

Technical methods have been proposed as alternative ways to deal with unlawful content. This involves the ISPs using filtering techniques to look inside the data packets to inspect the content. Known as "deep packet inspection", this entails the ISP opening the packets of data, and looking at what is inside, rather like the post-office opening every envelope to check for a CD. It is the same underlying technology that the Chinese use to censor Internet content. It is technically interception and raises serious questions related to privacy as well as censorship. There is a high risk of false positives and blocking of activities and content that is not unlawful. The use of deep packet inspection to control content has been rejected in the US by the FCC (see our comments below on the Comcast case (p. 3)).

Undesirable content: Asking an ISP to deal with undesirable content, results in the ISP making choices on behalf of its subscribers and it could amount to a form of censorship. Undesirable content is best dealt with by the individual consumers, who may purchase what is known as "parental control" software, which they may set to suit their own ethics, morals, religion and tastes. We maintain then that in such cases self-regulation is best, as it allows censorship at the receiving end and not at the source.

Further comments on the civil liberties issues: In a democratic legal system, it is the role of the court to be arbiter as to what is lawful or unlawful, and to impose sanctions. Giving ISPs the power to intervene directly without a sentence or injunction of a court in cases of alleged copyright infringement, contravenes some fundamental principles of UK law, and raises civil liberties questions for policy-makers. For example, it could mean that the ISP in question is acting as a policeman, judge and jury, or that it is acting on information from third parties. Graduated response measures raise concerns including that of a parallel justice system (where sanctions are imposed by private entities and not by a court) and commercial censorship. Either way, it will be viewed by the public as unacceptable.

We draw attention to the UK Human Rights Act. It is arguable that the Human Rights Act 1998 (HRA) recognised essential constitutional rights in the UK by adopting the European Convention of Human Rights (ECHR). We refer specifically to Article 10 of ECHR regarding the principle of freedom of expression as enshrined in section 12 of the Statute, and the right to a private life and correspondence privacy recognised by Article 8 of the ECHR. In doing so, HRA explicitly recognises that intrusion in the life of British citizens should be allowed only in exceptional cases which relate to the interests of national security, public safety or the economic well being of the country. We believe it is against the Act to confer ISPs -private institutions that are by no means "public authority"- the power to intrude on the privacy of British citizens.

In this regard, we also draw attention to the EU Telecoms Package and the amendment known as Amendment 138, which states that no restriction on these fundamental rights may be made without a court order. [5]

For policy-makers, the issues include: Under what criteria should data packets be intercepted and inspected and who should determine the criteria? How should ISPs be regulated for this kind of behaviour – does it merit audits? What processes should be in place to protect a) consumers b) owners of websites, services, and applications? What is the risk that the ISPs become the gatekeepers for the democratic media as well as e-commerce, entertainment, and other web activities (see further comments below)?

Question 5

Once again, this question is addressed in two parts.

Who should be paying for the transmission of Internet traffic?

From a policy perspective, the question raises issues for media policy in addition to telecommunications policy, and the issues are complex.

Currently, users pay for transmission – users, meaning the consumer or end-user, who pay for connections to the Internet, as well as the owners of websites and servers who pay for bandwidth so that people can access their server.

The open character of the Internet, which lowers the barriers for media distribution, has permitted the growth of many new niche players, who would not have had the opportunity otherwise, as well as the rise of the citizen journalist/blogger or film-maker (so-called user-generated content). Internet traffic comprises many different activities. Importantly, traffic may relate to e-commerce, as well as to business and trading activities of all types, as well as news media, entertainment and games, reflecting the same spread that exists off-line. Likewise, it reflects the broad spread of off-line social activities. This diversity of use is what makes the Internet special, and arguably, why there are civil liberties implications for policy-makers if this open character is compromised by altering the commercial structure of the Internet.

In terms of media content, there is a wide range of user-generated content and relatively inexpensive commercial content (such as news and sports) available online. The economic issue relates to the production of high quality expensive programming (e.g. films, drama) and it is arguable that content creators are still looking for a viable business model. The question here for policy-makers is whether to ask the content producers to contribute towards transmission costs, or conversely whether network transmission providers should be asked to contribute towards content creation costs, as recently introduced in France by the reform of the Public Sector Audiovisual scene.[6]

Would it be appropriate to enshrine any of the various notions of Network Neutrality in statute?

In a word, yes. Network neutrality refers effectively to treating all internet traffic equally. The alternative is to allow network operators and ISPs to prioritise certain types of traffic and discriminate against other types. As the Internet has grown over the years to become an essential part of the everyday life of the majority of the population, and as the amounts of data travelling on the internet have massively increased, there is an argument that network operators need to manage traffic in order to guarantee a certain level of service in terms of quality and security. That argument, valid as it may be, should not allow network operators to turn into gatekeepers of internet content (e.g. text, video or audio on a website), services (e.g. e-commerce), and applications (e.g. user-generated content sites). Clearly, if network operators were to effectively police the internet that would seriously damage not only market competition, economic growth, and innovation (much of which is done "at the edge of the network" and not centrally, and without requiring approval from network providers) but also civil rights, since a network operator would decide (on what basis?) which types of content, services, and applications its customers were allowed to access. It is for these reasons that we believe that network neutrality should be enshrined in statute with a specific reference to abuse of market power.

Related to this point, is the question of whether governments should intervene or whether they should let competition authorities deal with any issues as and when they arise. Effectively, the absence of network neutrality is about a provider with significant market power in the broadband access market leveraging power in the neighbouring markets for the provision of content, services, and applications. Whilst competition authorities have a role, we believe that the ex-post character of such interventions may adversely impact upon the market and we are therefore in favour of the network neutrality principle to be enshrined in statute in order that the sectoral regulator Ofcom would be empowered to intervene if and as needed in a timely manner.

Another recommendation we would like to put forward draws on developments in the USA. As the Comcast case clearly illustrated,[7] network providers need to disclose to both regulators and their customers their traffic management methods. Such disclosure will help customers make informed decisions and thus benefit from market competition, but also help regulators check against possible abuses of network management tactics.

Finally, a point of clarification. Some proponents of network neutrality argue that if it were to be abolished, the result would be price discrimination: network providers would be able to charge certain users more for faster connections and/or access to more content, services, and applications (premium service), and charge the rest a smaller fee for relatively slower connections and access to fewer content, services, and applications. However, price discrimination based on connectivity already exists in competitive markets. Internet broadband providers offer the option of

different connectivity packages (e.g. different download and/or upload limits) to their customers for different prices. We are not against that. Indeed, Internet users should have the option between lower price and lower quality service, or higher price and higher quality service. Greater choice and customised offerings are at the heart of market competition. Uniform prices then is not the reason we support network neutrality. We argue that it is appropriate to enshrine network neutrality in statute only because, as explained above, not doing so would have serious implications for economic growth and civil rights.

We also recommend the guidelines drawn up by the Norwegian Post and Telecommunications Authority which provide a concise but informed view on the issues surrounding network neutrality from a regulatory perspective.[8]

Specific comments related to the EU Telecoms Package and net neutrality: The EU Telecoms Package is a review of the EU telecommunications framework law. It raises net neutrality issues, in that the "compromise" text as voted in the European Parliament on 6 May 2009, contains Articles which *de facto* permit the prioritisation and discrimination against certain types of traffic, as outlined above; and it contains only very weak powers for regulatory intervention and instead relies on competition law, which, as we have suggested, may adversely impact on the market.

The current legal position is that the prioritisation of content, or discrimination against it (blocking) is neither permitted nor forbidden. The law says nothing about it, because when the current EU framework was drafted in 2002, such practices were not really possible. Now, with new technology known as traffic management systems, broadband providers may selectively block traffic. The Telecoms Package does not change this situation, but it does legitimise it. It says that blocking is fine as long as the operator says so, somewhere in the contract. That is very low legal barrier.

Current examples of discriminatory practice are the widely publicised case of T-Mobile blocking Skype on wireless access (note that wireless access from a laptop computer could be a user's main form of Internet access) and the blocking of peer-to-peer traffic. Peer-to-peer is used for non-entertainment purposes, and is used by new legal entertainment services which compete against the services offered by some providers - see our example of the FCC case referred to above, where the complainant offers legally licenced peer-to-peer television services.

For policy-makers, there are issues related to media policy and to commercial censorship. What happens when the CEO of a broadband provider makes a call to the network manager and asks for a change to the database, to block or slow sites that s/he is politically opposed to? Such moves could be very difficult to detect even with specialist expertise and technical tools. What happens when people are sold packages with a limited access (on the basis that "they only need this and this, and don't need to pay more")? They then will not be able to access many services which could benefit them. Conversely, owners of web-based services and e-commerce sites will lose out because they will find themselves with a smaller addressable market.

References

[1] The 2002 Regulations limit the liability of service providers who transmit or store unlawful content provided by others. It distinguishes among three categories of service providers : those who transmit information ("mere conduits"), those who engage in "caching" information, and those engaged in "hosting" information.

[2] For defamation cases, see for example *Godfrey v Demon Internet Limited* [1999] EWHC QB 244 and Bunt v Tilley, Hancox, Stevens, AOL, Tiscali and BT [2006] EWHC 407.

[3] 1988 Copyright Designs and Patents Act.

[4] Loi favorisant la diffusion et la protection de la Creation sur L'Internet (Creation and Internet law).

[5] Framework Directive, Article 8.4 (h)

[6] Act number 258 of 2009.

[7] In August 2008, the FCC ruled that Comcast, providing broadband connection to nearly 14.5m homes, behaved in an anti-competitively and discriminatory manner since, under the pretext of traffic management, it was secretly blocking certain bandwidth-hungry applications provided by its competitors (especially peer-to-peer applications). Available at < http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf>

[8] Network Neutrality, Guidelines for Internet Neutrality 24 February 2009.