The legality of deep packet inspection

Angela Daly[1]

Department of Law
European University Institute
Villa Schifanoia
Via Boccaccio 121
50133 Florence
Italy

email: Angela.Daly@eui.eu
tel: +393926465899

Abstract

Deep packet inspection is a technology which enables the examination of the content of information packets being sent over the Internet. The Internet was originally set up using "end-to-end connectivity" as part of its design, allowing nodes of the network to send packets to all other nodes of the network, without requiring intermediate network elements to maintain status information about the transmission. In this way, the Internet was created as a "dumb" network, with "intelligent" devices (such as personal computers) at the end or "last mile" of the network. The dumb network does not interfere with an application's operation, nor is it sensitive to the needs of an application, and as such it treats all information sent over it as (more or less) equal. Yet, deep packet inspection allows the examination of packets at places on the network which are not endpoints. In practice, this permits entities such as internet service providers (ISPs) or governments to observe the content of the information being sent, and perhaps even manipulate it. Indeed, the existence and implementation of deep packet inspection may challenge profoundly the egalitarian and open character of the Internet.

This paper will firstly elaborate on what deep packet inspection is and how it works from a technological perspective, before going on to examine how it is being used in practice by governments and corporations. Legal problems have already been created by the use of deep packet inspection, which involve fundamental rights (especially of Internet users), such as freedom of expression and privacy, as well as more economic concerns, such as competition and copyright. These issues will be considered, and an assessment of the conformity of the use of deep packet inspection with law will be made. There will be a concentration on the use of deep packet inspection in European and North American jurisdictions, where it has already provoked debate, particularly in the context of discussions on net neutrality. This paper will also incorporate a more fundamental

1 PhD Candidate, Department of Law, European University Institute; LLM 2007, Université Paris 1 Panthéon-Sorbonne; BA (Hons) 2006, University of Oxford. A version of this article was presented at the First Interdisciplinary Workshop on Communications Policy and Regulation 'Communications and Competition Law and Policy – Challenges of the New Decade', University of Glasgow, 17 June 2010.

assessment of the values that are desirable for the Internet to respect and exhibit (such as openness, equality and neutrality), before concluding with the formulation of a legal and regulatory response to the use of this technology, in accordance with these values.

1. Introduction

In the Internet's twenty years of being available as a mass public medium there have been various developments and changes as regards the technologies involved, as well as the types of actors, whether public or private, taking an interest in it. Indeed, the current state of the Internet is a far cry from the cyberlibertarians' description of it in the 1990s as being unregulable, uncontrollable and indomitable – governments of both authoritarian regimes and liberal democracies have been able to assert varying degrees of legal and political control over the medium,[2] as well as large Internet corporations such as Google forming, and pre-existing commerce entering the Internet arena. Although the Internet as a whole is not controlled or regulated by any one person, organisation, company or state, power can be asserted at the different levels of the Internet's architecture: hardware, software, ISPs, content providers, search engines and users.

Internet provision is the basic and most fundamental level of the Internet, as all other levels are dependent upon it: without a connection to the Internet, it is impossible to create content to put online in the hope that it will feature highly in Google's search results, download music from social networking website, or keep up-to-date with the latest news on political blogs.

Internet access in the developed jurisdictions considered in this paper is generally provided to users by private telecommunications companies;[3] in countries where there used to be a state telecoms monopoly, the incumbent operators still occupy a major, if not dominant, position in the telecoms markets (including that of Internet provision) of their respective countries, and often own much of the telecoms infrastructure.

Deep packet inspection (DPI) is a technology deployed at the level of Internet provision to decipher the content of the information that is travelling through the network, and has been employed by governments and corporations to regulate and control the flow of information across the network for various ends. This paper will explore the uses of DPI and their compliance with the law: given the way Internet provision is structured, there is the potential for a technology such as DPI to be used abusively as regards Internet users. Whether this is happening, what the current legal response is, and whether that is sufficient and appropriate will be determined here.

2. The technology of deep packet inspection

The Internet was set up using "end-to-end connectivity" as part of its design, allowing nodes of the

2 For a detailed account of this, see JACK GOLDSMITH & TIM WU WHO CONTROL THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD *(*2006).

3 Although there has been some government activity in this area in some countries, such as the National Broadband Plan launched by the American Federal Communications Commission (FCC) which includes the goal of universal access to broadband Internet, entailing the creation of various funds to finance this. For more information see: http://www.broadband.gov (last visited 3 June 2011).

network to send packets to all other nodes of the network, without requiring intermediate network elements to maintain status information about the transmission. This is implemented in the TCP/IP protocols. What this means is that the Internet was created as a "dumb" network, with "intelligent" devices (such as personal computers) at the end or "last mile" of the network. The dumb network does not interfere with an application's operation, nor is it sensitive to the needs of an application, and in this way it treats all information sent over it as equal. In such a network, the content of the packets is not examined, and Internet providers act according to the destination of the data as opposed to any other factors.

Deep packet inspection involves inspection points being set up at some point in the network which is not an end-point which look into the content of the packets being sent over the network, and act on that information in accordance with whether it conforms to established criteria. Using DPI, the owner of the network infrastructure is able to manipulate what information is received over the network.

There have been predecessor technologies to DPI, namely shallow packet inspection (also known as "stateful packet inspection") and packet pre-filtering.[4] Shallow packet inspection examines the headers of the packets (which is the information placed at the beginning of a block of data, such as the sender and recipient's IP addresses), as opposed to the body or "payload" of the packet. This kind of packet inspection allows the communications to remain 'virtually anonymous' since the content of the packets is not observed, and the information in the header used only to route the packet.[5] Packet pre-filtering involves filtering out a few, suspicious packets while letting the majority of packets through unchecked. Bendrath acknowledges a major limitation of these technologies in filtering, that 'it can be useful if there is a list of known terms and regular expressions to looks for, like virus and mal-ware signatures, but is less useful when filtering is supposed to be based on behavioural information'.

Bendrath believes DPI exhibits many functions which have been previously available, but also two 'interesting and potentially paradigm-changing characteristics', namely the possibility to analyse and discriminate Internet traffic in real time, and 'the integration of these diverse functions into one piece of equipment', only available now as a result of recent advances in computer engineering. This makes monitoring and manipulation in the form of blocking or discriminating against information as it is being sent over the Internet more easy and effective than with previous technologies.

3. Uses of deep packet inspection

DPI is being used by public and private entities to view the contents of packets of information being sent over the Internet, and act in various ways on this information. Despite the range of current uses of DPI, it was originally intended as a means of managing the network to safeguard Internet users from malicious programmes being sent over the Internet by intercepting them before they reached the end-users. While this remains one function of DPI, the technology has also been put to other

4 Ralf Bendrath, Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection, Paper prepared for the International Studies Annual Convention New York City 15-18 February 2009, p14 Available at: http://userpage.fu-berlin.de/~bendrath/Paper_Ralf-Bendrath_DPI_v1-5.pdf (last visited 3 June 2011).

5 Andrea N. Person, Behavioural Advertisement Regulation: How the Negative Perception of Deep Packet Inspection Technology May be Limiting the Online Experience Fed. Comm. L.J. 62, 436. Available at: http://www.law.indiana.edu/fclj/pubs/v62/no2/11-PERSON_FINAL.pdf (last visited 3 June 2011).

uses, such as network management, government surveillance, targeting advertising and dealing with copyright infringements. These uses in North American and European jurisdictions will be considered below.

Network security

As mentioned above, DPI was originally developed to secure local area networks (LANs), which are used to cover small geographical areas such as a company or university, in order to ensure there is no unwanted traffic coming in from outside the network. This task used to be accomplished by firewalls, but due to developments in Web applications the delimitation between the internal LAN and the external Internet is not so well-defined, and so network administrators must now fully inspect the data coming in and out of the LAN to achieve this. The provision of network security by DPI is only used by these internal private networks, and not by ISPs providing Internet access to end-users due to the ISP being able to externalise the users' security problems. In addition, DPI can be used in such networks to prevent sensitive data from being leaked by people internal to the network to the outside world, for instance by being able to detect when a user is trying to send a protected file outside of the network.

Government surveillance

DPI has also been used by the US government to monitor and censor the information American citizens are receiving and disseminating over the Internet. So far there appears to be few known instances of DPI being used by governments in Europe, although that may just be due to such instances not yet having been brought to light.

In the US, DPI is used to enable ISPs to comply with the 1994 Communications Assistance for Law Enforcement Act (CALEA),[6] which requires telecommunications carriers to ensure that their equipment and services have in-built surveillance capacities to allow federal agencies to monitor communications in real-time for the purposes of criminal investigations. As per a 2005 FCC Order, providers of broadband Internet and Voice over IP (VoIP) services constitute 'telecommunications carriers' under the CALEA, such that Internet traffic as well as traditional phone calls could be surveilled.[7] Given a lot of DPI equipment also complies with CALEA, it is used to enable these providers to conform to the legislation.

In the US context, Bendrath also highlights various instances of less legal uses of DPI by government bodies such as the National Security Agency via ISPs, with an ostensible justification for this being the War on Terror. When the Electronic Frontier Foundation (EFF) sued AT&T for its participation in illegal spying contrary to the Foreign Intelligence Surveillance Act (FISA), but Congress passed the FISA Amendments Act which granted immunity to telecoms firms which participated in the wiretapping initiative, and so a federal judge dismissed the case.[8] EFF wanted to appeal the decision to the Ninth Circuit Court of Appeal, arguing that the FISA Amendments Act was unconstitutional due to it 'granting the president broad discretion to block the courts from considering the core constitutional privacy claims of millions of Americans'. However, the case was

6 Nate Anderson Deep packet inspection meets 'Net Neutrality, CALEA, Ars Technica (25 July 2007), http://arstechnica.com/civis/viewtopic.php?f=2&t=23567&p=495523 (last visited 3 June 2011).

7 Federal Communication Commission CALEA First Report and Order, 23 September 2005. Available at: hraunfoss.**fcc**.gov/edocs_public/attachmatch/**FCC**-05-153A1.pdf (last visited 3 June 2011).

8 For more information see: http://www.eff.org/nsa/hepting (last visited 3 June 2011).

returned to the District Court by virtue of the FISA Amendments Act, which eventually dismissed it in 2009, seemingly rejecting the unconstitutionality argument and accepting the government's justification that AT&T's behaviour was 'lawful' because it was designed to prevent, even indirectly, a terrorist attack.

Network management

ISPs have been using DPI for the purpose of "network managements", which incorporates various functions such as ensuring a basic quality of service (QoS) for the end-users, preventing congestion on the network, and facilitating the creation of different packages of Internet access for consumers ("access-tiering"). Bendrath characterises this use of DPI as a combination of 'technological efficiency' and 'economic interests'. The most principled justification for ISPs to use DPI here is that of guaranteeing a certain QoS level and avoiding network congestion: users using high-bandwidth applications which congests the network ought to pay more to do this, or alternatively these applications will be blocked, as otherwise the ISP cannot provide a good service to its customers not using such applications. Yet, even if this is the case, it is unclear how much more investment in the network infrastructure would be needed for high bandwidth applications not to pose such a problem, as ISPs when making such assertions have tended not to offer a very detailed justification of why this is the case. Research from the Internet Society (ISOC) seems to suggest that network capacity is growing by about 50% each year, so 'there does not seem to be a problem in catering to Internet traffic growth, at least at the macro level'.[9] Bendrath broadly agrees with this assessment of network capacity, but he argues that 'the last mile has become a bottleneck due to the growth of these bandwidth-consuming applications'.

In the USA, the cable operator Comcast began to block peer-to-peer (P2P) data transfers for its users using DPI. This resulted in the Federal Communications Commission (FCC) ordering Comcast to 'end discriminatory network management practices', since it had 'unduly interfered with Internet users' right to access the lawful Internet content and to use the applications of their choice',[10] starting a lengthy legal process over whether the FCC was legally capable of issuing such an order, and catalysing the general debate in the US on net neutrality.

The issue has not been restricted to the US. In Canada, the use of DPI in network management has had overt free expression implications, namely the case of communications provider Telus blocking its subscribers' access to a website run by Telecommunications Workers Union members in July 2005.[11] Furthermore, in 2008 the major telecommunication company Bell Canada was found to have been engaging in Internet traffic "shaping and throttling", but the Canadian Radio-television Telecommunications Commission (CRTC) did not sanction it due to Bell Canada demonstrating a need to engage in this behaviour because of congestion in the network, and the fact it was done in a way that did not discriminate between its own retail end-users, and the end-users of other ISPs[12]. However, the CRTC also issued a notice on the same day, consulting on the traffic management practices of ISPs[13] in order to deal with some of the more general contentions made by parties to the

9 Mat Ford, The Bandwidth Bandwagon, IETF Journal 5, 3 (2010).

10 The full text of the FCC's press release can be found as a link on this page: http://www.fcc.gov/Daily_Releases/Daily_Digest/2008/dd080804.html (last visited 3 June 2011)

11 CBC News Telus cuts subscriber access to pro-union website (24 July 2005), http://www.cbc.ca/canada/story/2005/07/24/telus-sites050724.html (last visited 3 June 2011).

12 Telecom Decision CRTC 2008-108. Available at: http://www.crtc.gc.ca/eng/archive/2008/dt2008-108.htm

13 Telecom Public Notice CRTC 2008-19. Available at: http://www.crtc.gc.ca/eng/archive/2008/pt2008-19.htm

decision on Bell Canada's conduct.

While not as prominent as in North America, concerns generated by the use of DPI in network management have also been relevant in Europe. For example, in April 2008 the CEO of Virgin Media, Neil Berkett, claimed content providers who would not pay Virgin Media for faster access 'might end up in slower "bus lanes"'.[14] Indeed, Person states that the practice of tiering is 'common' in the UK, 'where services like PlusNet sell broadband accessibility by the gigabyte and pair routers with varying degrees of capacity to the type of bandwidth the user purchases'.

This use of DPI to slow or block certain types of Internet traffic has given rise to the debate over whether a principle of net neutrality should continue to define the Internet. Such a principle would prevent ISPs from discriminating between different kinds of Internet traffic, and the restriction of content, sites or platforms (at least those which are legal). Prior to network management practices facilitated by DPI, there had been a general principle of net neutrality as the default position governing Internet traffic, and net neutrality proponents advocate that this should remain the case.

Targeted advertising

DPI has enabled organisations to target advertisements to Internet users depending on their interests, which are defined according to the users' web-browsing habits. Data on what users are looking at on the Internet is gathered by ISPs, which is analysed and used to show individualised advertisements which 'follow users across the Internet and directly pertain to his or her demonstrated interests'. This approach to advertising to users based on their conduct on the Internet is known as 'behavioural advertising'. ISPs are particularly well-placed to facilitate this kind of advertising given 'they have access to all their subscribers' web surfing data, because they are the one[s] who transport all their internet traffic'. So far, targeted advertising has mainly been used in the US and UK.

Targeted advertising using DPI has a predecessor technology in the form of "cookies". Cookies work by storing information on a user's web browser, which is sent back to the web server from which it originates each time the browser accesses that server. Websites can then use cookies to gather information about users and their browsing habits. However, there is an important limitation of cookie technology as compared to DPI, which is that cookies are only able to access a predetermined amount of information. In contrast, everything that a user is doing on the Internet is accessible via DPI.

A prominent example of the use of DPI to effect targeted advertising is that of the partnership between the UK ISP British Telecom (BT) and Phorm, an American firm which provides advertising software. In 2007 BT controversially trialled Phorm's adware technology on ten of thousands of BT customers without their knowledge or consent.[15] The following year the companies conducted another trial in a more transparent fashion: 'sensitive' websites were not used to form user profiles, customers were to opt-in to the trial, and conducted an analysis of the impact of the trial on users' privacy.

Copyright infringements

14 Royal Television Society Television Magazine Pay-per-voom TV, 45.4 April 2008.

15 Chris Williams BT's 'illegal' Phorm trial profiled tens of thousands, The Register (14 April 2008), http://www.theregister.co.uk/2008/04/14/bt_phorm_2007/ (last visited 3 June 2011).

Copyright holders have been requesting the use of DPI by ISPs to prevent copyright infringement and enforce their rights in both Europe and the US. There has been litigation in European Member States such as Belgium and Ireland to attempt to establish the liability of ISPs for customers who are illegally sharing copyrighted material, although the Belgian case was settled out of court when the technology suggests by the Belgian music industry association SABAM was found not to be effective in detecting such copyright breaches, and subsequently the parties in the Irish case negotiated an agreement to disconnect users from the Internet after they have been found to have been illegally distributing music on three occasions.[16]

In the US, ISPs currently enjoy a status which exempts them from liability for carrying illegal or illicit content, due to section 509(c)(1) of the Communications Decency Act.[17] Pre-DPI, it seems that ISPs qualified for a "safe harbour" from copyright liability due to section 512(k)(1)(A) of the Digital Millennium Copyright Act (DMCA), which protects 'service providers' from liability so long as they do not modify the content of the material being sent or received. Case law from before and after the enactment of the DMCA has exempted ISPs from copyright liability so long as they do not themselves induce the copyright infringement. Friedan argues that it is possible that ISPs which use DPI to engage in network management for *inter alia* the purpose of increasing their profit no longer operate as neutral conduits of information lacking knowledge of the material being sent over their networks, and so may no longer qualify for this exemption. Friedan also explores whether the availability and *de facto* legality of DPI entails the obligation on ISPs to use it in detecting copyright infringements, and concludes that the DMCA does not currently require this, but it may in the future when 'ISPs readily can use deep packet inspection to perform traffic and QoS tiering as well as copy protection as standard operating procedure', a scenario which would seem to be coming to pass 'in light of the promising array of DRM, traffic management, and service diversification options offered by next generation Internet routers'.

Although an obligation for ISPs in the US to use DPI for copyright infringement purposes does not seem to exist, there have been instances of ISPs voluntarily using DPI for this reason, such as AT&T announcing in January 2008 that it would inform copyright holders if it detected an infringement occurring on its network, and would even suspend the Internet connection of customers violating copyright in this way.

4. Deep packet inspection and the law

The preceding discussion of the uses of DPI in North American and European jurisdictions prompts an analysis of the legality of these uses. There are four areas in which the use of DPI may not be in conformity with legal provisions in these jurisdictions: privacy; free expression; competition; and due legal process.

16 Indeed, recent legislation in France in the form of the HADOPI law, and in the UK in the form of the Digital Economy Act has formalised this approach to copyright infringement, and provides that the connections of users who persistently infringe copyright can be suspended temporarily. However, the use of DPI seems not to be considered, as copyright holders are to inform ISPs when there has been a copyright infringement, and only then are ISPs required to contact the user to inform her that she has violated copyright. This can be achieved by the ISPs matching the IP address to the real name and geographical address of its subscriber. Nevertheless, DPI would be a more efficient method of doing this.

17 Rob Frieden, Internet Packet Sniffing and its Impact on the Network Neutrality Debate and the Balance of Power between Intellectual Property Creators and Consumers (June 2007), http://ssrn.com/abstract=995273 (last visited 3 June 2011).

Privacy

The uses of DPI seem to generate *prima facie* privacy concerns, as data about users' behaviour on the Internet (which could also include sensitive data) is being monitored and used for various purposes. Indeed, the examination above of uses of DPI for government surveillance and targeted advertising already demonstrate the privacy concerns involved with this technology.

As mentioned above, in the *Hepting* litigation, the EFF alleged that the FISA Amendments Act protecting the US federal government's use of DPI for intercepting citizens' communications is unconstitutional, being contrary to the Fourth Amendment to the Constitution, which protects citizens against 'unreasonable searches and seizures'. Since *Katz v United States,*[18] government intrusion using technology has also constituted a 'search' for the purposes of the Fourth Amendment (in that particular case, wiretapping), so it would appear that governmental monitoring of Internet traffic would also fall within the remit of Fourth Amendment protection. Whether the interference in citizens' privacy is reasonable or not would seem to depend upon the circumstances of the case. Given the large amount of American citizens whose communications were being monitored, it being quite likely that the majority were not involved in terrorist or criminal activities, and the broad discretion effectively being granted to the US President by the FISA Amendment Act, then this intrusion into citizens' privacy may well be considered to be 'unreasonable', although in practice the litigation saga concluded with the District Court justifying the US Government's behaviour by appealing to concerns over terrorism.

In Europe, privacy is protected by Article 8 of the European Convention on Human Rights (ECHR), an obligation primarily pertaining to contracting States, although the European Court of Human Rights (ECtHR) has interpreted it broadly. It is also protected by the EU's Data Protection Directive,[19] which regulates the processing of personal data and pertains to organisations in the private as well as public sector. If personal data is to be processed, it must be done transparently (i.e. by informing the data subject and seeking her consent before her data is processed), for a legitimate purpose and conform to the principle of proportionality. As a general point, the use of DPI in Europe by governments or private entities would have to comply with these requirements.

Regarding the use of DPI for targeted advertising, in response to the BT Phorm trials, the European Commission opened an infringement proceeding against the UK regarding the use of this software, after having received complaints from British Internet users, alleging the UK had not complied with European rules on the confidentiality of communications.[20] In September 2010, the Commission referred the case to the European Court of Justice since no changes to UK law to implement the EU rules fully were made as a result of the investigation.[21] At the time of writing, the case is ongoing.

---

18 389 U.S. 347 (1967)

19 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data. More information on data protection in the European Union can be found at: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm (last visited 3 June 2011).

20 European Commission press release Telecoms: Commission launches case against UK over privacy and personal data protection *(*14 April 2009), http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570 (last visited 3 June 2011).

21 European Commission press release Digital Agenda: Commission refers UK to Court over privacy and personal data protection (30 September 2010), http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1215&format=HTML&aged=0&language=EN&guiLanguage=en (last visited 3 June 2011).

In the US, there is currently litigation in the form of a class action about the use of software similar to Phorm's provided by NebuAd to the ISP WideOpenWest (WOW!) to conduct targeted advertising in 2008, with the contention that the use of this software violated privacy laws. The targeted advertising service was provided to WOW! Customers on an opt-out basis. The litigation was initiated in late 2008 in a federal court in California, which dismissed the case in 2009 due to a lack of jurisdiction. The case was then re-filed in late 2009 in the District Court for the Northern District of Illinois. In 2011, the District Court for the Northern District of California denied NebuAd's motion to dismiss the case, finding that the plaintiff had sufficient standing in the action.[22]

Free expression

ISPs' use of DPI to facilitate the management of their networks in a non-net neutral fashion has been viewed as detrimental to good conditions for free expression on the Internet. Indeed, Wu has advocated an enacted net neutrality principle 'to forbid broadband operators, absent a showing of harm, from restricting what users do with their Internet connection',[23] thus facilitating and protecting users' free expression on the Internet.

American scholars Lessig and McChesney identify various free expression issues pertaining to network management. They see access-tiering as a particular concern in the absence of net neutrality rules, asserting that 'firms would be able to sell access to the express lane to deep-pocketed corporations and relegate everyone else to the digital equivalent of the winding dirt road', warning that in this case the Internet will 'start to look like cable TV – a handful of massive companies would control access and distribution of content, deciding what you get to see and how much it costs'.[24] Given the Internet's previous record on facilitating free expression of individuals, which was restricted to a much greater extent in the traditional one-way broadcasting world, it would be a great loss if the Internet was to mimic this model, with its associated disadvantages for free expression. Indeed, corporate control over what information users create, disseminate and receive could also entail access to content or programmes which are not commercially lucrative is restricted only to those willing to pay more to the ISP to access it, or not available at all. In addition, it would seem that the legal protection of free expression in the US, namely the First Amendment to the Constitution, would not be effective in this scenario, since the First Amendment has been historically conceptualised as a right to free expression to be enforced against government interference, but not as against other private, non-state actors, such as private companies. Indeed, in the US (unlike in Europe), private companies may also be entitled to First Amendment protection, which may mean that not only can users not enforce their right to free expression against such entities, but also that the behaviour of such corporations in 'managing' Internet traffic using DPI may itself be constitutionally protected.

In the European context, Chirico, Van der Haar and Larouche acknowledge end-users' and content providers' 'fundamental right to receive and impart information, enshrined inter alia in Art 10

22 Mali Friedman California Privacy Claims Survive Motion to Dismiss in NebuAd Lawsuit Inside Privacy (3 May 2011), http://www.insideprivacy.com/united-states/california-privacy-claims-survive-motion-to-dismiss-in-nebuad-lawsuit/ (last visited 3 June 2011).

23 Tim Wu Network Neutrality, Broadband Discrimination, Journal of Telecommunications and High Technology Law, 2, 141 (2003).

24 Lawrence Lessig & Robert W. McChesney, No Tolls on the Internet, Washington Post (8 June 2006) available at: http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/AR2006060702108.html (last visited 3 June 2011).

ECHR'[25], with the implication being that this could come into conflict with non-net neutral conduct from ISPs. However, Art 10 of the ECHR is an obligation primarily pertaining to contracting States, and is usually conceived of as a negative freedom. Furthermore, enforcement of Art 10 may not be consistent across contracting States, and effective enough to ensure net neutrality. Nevertheless, Art 10 has been found to have some horizontal, positive effect in the case of Khurshid Mustafa and Tarzibachi v Sweden, a dispute between tenants and their landlord over a satellite dish the tenants had installed to receive Arabic and Farsi language programmes against the terms of the tenancy agreement. In this case, the European Court of Human Rights (ECtHR) found that the applicants' freedom to receive information via satellite broadcast, which formed part of Art 10, had been violated as the State, Sweden, had 'failed in their positive obligation to protect that right'. It is possible that the reasoning in this decision could also be applied to freedom to receive information on the Internet, which the behaviour of ISPs in using DPI (especially if it is being used to block certain information) may violate. Nevertheless, the process of enforcing ECHR rights is essentially an *ex post* procedure, where the right must first be violated, the individual whose right had been violated must first exhaust available national remedies before then taking a case to the ECtHR, a process which takes many years and can hardly be said to be an efficacious means of protecting free expression, especially in the context of a quickly-evolving technology such as the Internet.

There have also been various regulatory initiatives regarding net neutrality undertaken on both sides of the Atlantic in the last few years.[26] Some of the responses provide some guarantee for users to send, receive and use the content, services and applications of their choice over the Internet. This goes some way to fulfilling users' right to free expression online, but is not a full, enforceable guarantee of free expression as against ISPs using DPI.

In any event, it may well actually be desirable from a user's point of view for ISPs to use DPI to prioritise certain types of information being sent across the network, such as applications which are sensitive to delay or signal distortion (such as VoIP or video streaming) over applications which are not sensitive in these ways (such as email). Some network management to ensure a minimum QoS for these applications may merit legitimate restrictions on a net neutrality principle, as also acknowledged by Wu.

Competition

The use of DPI by ISPs also generates competition concerns. Since ISPs can use DPI to prioritise certain types of information travelling across the network, they could for example favour the content of their subsidiary (if there is vertical integration), or discriminate between different content providers e.g. in favour of a particular content provider if it pays the ISPs for faster access. This makes the assumption that there is economic dominance and/or oligopolistic behaviour in the markets for Internet provision, and that the market would not itself provide the solution to this problem.

In the US, Lessig and McChesney have asserted that the 'neutral' Internet network has guaranteed 'a free and competitive market for Internet content',[27] with the implication being that ISPs using DPI to behave in a non-neutral way could incidentally also be behaving in an anticompetitive fashion. In

25 Filomena Chirico, Ilse M. Van der Haar, & Pierre Larouche, Network Neutrality in the EU TILEC Discussion Paper No. 2007-030, http://ssrn.com/abstract=1018326 (last visited 3 June 2011).

26 For a detailed analysis of these measures, see: Angela Daly Regulatory Approaches to Net Neutrality in Europe and Beyond (2010), http://ssrn.com/abstract=1675744 (last visited 3 June 2011).

27 See supra note 24.

the EU, Chirico, Van der Haar and Larouche do not think this will be such as crucial issue there as in the US, with one of the reasons being that the EU broadband market is more competitive than that of the US. In the US, the regulatory approach has led to a duopoly of integrated broadband access providers,[28] whereas the European regulatory approach has been different, with more competitive wholesale and retail broadband markets, and ownership of the local path not being a barrier to entry on the retail market. Nevertheless, Chirico, Van der Haar and Larouche recognise some competition issues arising from ISPs' use of DPI to manipulate the flow of Internet traffic in the absence of net neutrality regulation in Europe. They acknowledge that it is possible that a vertically-integrated broadband provider may try to favour its subsidiary's content using DPI, but they think that this is unlikely to happen in practice, due to this kind of vertical integration historically not being found in the media sector,[29] regulation countering the market power of wholesale broadband providers with a competitive retail broadband market, and Art 102 preventing a dominant firm from discriminating in an up- or downstream market in favour of its subsidiary. They argue that blocking content may be a more serious problem, as a loss of economies of scale or network effects might result in a blocked content provider being excluded from the market altogether, such as one whose content is not commercially lucrative. There may be benefits for innovation, as broadband providers may be incentivised to invest in their own content, but they admit that this is unlikely to outweigh the disincentive to invest pertaining to independent content providers if they face the possibility of being blocked.

Again, the net neutrality regulation that has been enacted on both sides of the Atlantic has taken these competition concerns into account, by placing restrictions on the extent to which ISPs can discriminate against or in favour of certain types of traffic passing through their networks, as well as the outright blocking of traffic. In addition, the *ex post* residual competition regimes still apply.

Copyright and due process

The use of DPI by ISPs to prevent and sanction copyright infringement raises a fundamental question of due process. Copyright infringements are usually governed by civil as opposed to criminal law, and ought to be subject to judicial scrutiny. The use of DPI by ISPs to monitor whether Internet users are infringing copyright, and then suspending their Internet connection if the ISP deems them to be doing so would seem to violate the principle of legal due process, with the ISP taking on an unwarranted policing and judicial function. Indeed, the American Center for Democracy & Technology has recently been critical of such practices, whether mandated by governments or initiated by ISPs as being contrary to due process.[30]

5. Legal and regulatory response and reform

DPI is neither per se legal or illegal – the legality of DPI depends on who is using it, how it is being used and the purpose for which it is being used. The analysis of the uses of DPI in North America

28 Of which one is Comcast, which has already been using DPI to engage in non-net neutral behaviour. The other major provider is AT&T.

29 The authors seem to have overlooked the (ultimately unsuccessful) AOL Time Warner merger, a prominent case of vertical integration in the media sector.

30 Center for Democracy and Technology Copyright "Enforcement" Policies Could Have Broad Impact (4 May 2010), http://www.cdt.org/policy/copyright-enforcement-policies-could-have-broad-impact (last visited 3 June 2011).

and Europe contained in this paper suggest that there are two broad improvements which could be made when it comes to the legal use of DPI, falling under the headings of transparency and free expression.

Transparency

It seems that transparency tied to user consent is key to DPI being used legally. This can be seen from the discussion of alleged infringements of consumer privacy by ISPs using DPI: the fact that either DPI was being used without consumers' knowledge, or was being used on an opt-out rather than opt-in basis appears not to constitute sufficiently transparent use of the technology. If ISPs inform their customers of their use of DPI, and use it on an opt-in basis for customers, this would seem to constitute a more "legal" use of DPI. Nevertheless, especially when it comes to sensitive personal information, even if ISPs are more transparent about their use of DPI, this still may constitute privacy violations.

Furthermore, as regards network management, it seems that some use of DPI to prioritise some types of Internet traffic on a QoS basis would be desirable. However, given the potential (as well as actual) abuse of such a position of network control, it would be unwise to leave network management, even just vis-a-vis a minimum QoS solely to the ISPs. Indeed, the need for at very least increased transparency in this area is one topic on which all the regulatory responses to net neutrality formed so far agree: they all provide that ISPs must disclose information about the Internet connections that they are selling, (although some of the regulatory responses are more detailed than others, and the approach to transparency takes a more consumer protection than, e.g. free expression approach).

Free expression

Until an expansive interpretation of Art 10 ECHR in Europe is adopted and the right to free expression contained in the First Amendment to the US Constitution is formulated in the way Moran Yemini suggests,[31] free expression will not be adequately protected against infringing uses of DPI by ISPs. Since as explained above, the right to free expression is primarily conceived of in contemporary jurisprudence as a right against the government, and legal protections of free expression are formulated to reflect this. ISPs in the jurisdictions under consideration in this paper are private entities, and so are not *prima facie* under a legal obligation not to interfere with the free expression of their customers. An explicit and enforceable guarantee of the right to free expression of Internet users *vis-a-vis* their ISPs' network management practices would be highly desirable.

31 Moran Yemini, Mandated Network Neutrality and the First Amendment: Lessons from *Turner* and a New Approach, VA. J.L. & TECH 13, 1 (2008).