From porn to cybersecurity passing by copyright: How mass surveillance technologies are gaining legitimacy…
The case of Deep packet inspection technologies

Sophie Stalla-Bourdillon, Evangelia Papadaki, Tim Chown

Abstract
Recent coverage in the press regarding large-scale passive pervasive network monitoring by various state and government agencies has increased interest in both the legal and technical issues surrounding such operations. The monitoring may take the form of which systems (and thus potentially which people) are communicating with which other systems, commonly referred to as the metadata for a communication, or it may go further and look into the content of the traffic being exchanged over the network. In particular the monitoring may rely upon the implementation of Deep Packet Inspection (DPI) technologies. These technologies are able to make anything that happens on a network visible and recordable. While in practice the sheer volume of traffic passing through a DPI system may make it impractical to record all network data, if the system systematically records certain types of traffic, or looks for specific patterns in all traffic, the privacy concerns are highly significant. The aim of this paper is twofold: first, to show that despite the increasing public awareness in relation to the capabilities of Internet service providers (ISPs), a cross-field and comparative examination shows that DPI technologies are in fact progressively gaining legal legitimacy; second to stress the need to rethink the relationship between data protection law and the right to private life as enshrined in Article 8 of the European Convention on human rights and Article 7 of the European Charter of fundamental rights in order to adequately confine DPI practices. As a result, it will also appear that the principle of technical neutrality underlying ISP's liability exemptions is misleading.

Keywords: privacy, private life, data protection, data retention, deep packet inspection, interception, traffic data, metadata, monitoring, Internet service providers (ISPs)

Recent coverage in the press regarding large-scale passive pervasive network monitoring by various state and government agencies has increased interest in both the legal and technical issues surrounding such operations. The monitoring may take the form of which systems (and thus potentially which people) are communicating with which other systems, commonly referred to as the metadata for a communication, or it may go further and look into the content of the traffic being exchanged over the network.

Deep Packet Inspection (DPI) technologies are able to make anything that happens on a network visible and recordable. They are, therefore, of particular interest for both state and commercial actors, as a tool for monitoring citizens' and customers' behaviour. However, this also means that DPI technologies, just like CCTV or databases, can be conceived as surveillance techniques and including mass surveillance techniques in as much as they are "not targeted on any particular individual but gather images and information for possible future use".[1] Their generalisation could thus have serious repercussions for Internet users, in particular in terms of the right to private life and freedom of expression. While in practice the sheer volume of traffic

[1] House of Lords, Select Committee on the Constitution, "Surveillance: Citizens and the State" (2nd report of session 2008-2009), February 2009, accessed February 25, 2014, http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf, p. 12.

passing through a DPI system may make it impractical to record all network data, if the system systematically records certain types of traffic, or looks for specific patterns in all traffic, the privacy concerns are highly significant.
Consequently, it is crucial to identify the implications of the technology being developed in order to make sure adequate safeguards, including legal safeguards are complied with, assuming there is a will to enforce them. This is all the more true that since the inception of the Internet it has proved very challenging to apply existing legal rules to an evolving technological environment in a well-informed way. The legal scrutiny of DPI technologies shows this perfectly.
The aim of this paper is twofold. First of all, to show that despite the increasing public awareness in relation to the capabilities of Internet service providers (ISPs), which has had the consequence of reducing the popularity of DPI technologies among ISPs[2] and thereby its overall use in 2012, a cross-field and comparative examination shows that DPI technologies are in fact progressively gaining legal legitimacy. Second to stress the need to rethink the relationship between data protection law and the right to private life as enshrined in Article 8 of the European Convention on human rights (ECHR) and Article 7 of the European Charter of fundamental rights in order to adequately confine DPI practices. As a result, the horizontal regime of exemptions of liability set up by the Directive on e-commerce[3] and grounded on the assumption that mere conduits' activity "is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored"[4] appears slightly misleading and should certainly be balanced with the setting up of mechanisms to prevent the creeping extension of surveillance practices. For this purpose it is suggested that the criteria of "retention of data" and "behaviour modification" (e.g. blocking access to certain webpages or files) are of primary relevance to justify the implementation of DPI practices.
The demonstration will proceed in three parts. Part A will give a brief overview of the technology at stake. Part B will show that when the goal pursued is content regulation the legal scrutiny deployed to assess the validity of the act of implementing DPI technologies is not very demanding and in particular give little weight to privacy interests. It is therefore unsurprising that the UK legislator has recently attempted to legitimize the use of DPI for accessing "third-party communications data" by law enforcement agencies. Part C will then attempt to illustrate the interplay between data protection law and DPI to demonstrate that up until now data protection law has offered little resistance to the implementation of DPI for monitoring and behaviour modification purposes, while identifying at least three routes to refine the existing regulatory framework.
Not to be misleading, the focus of the this paper is set upon ISPs' DPI practices and not law enforcement agencies' DPI practices, such as the US National Security Agency or the British Government Communications Headquarters. Its main aim is to examine how judges have dealt with the legal implications of the implementation of DPI technologies and to test the appropriateness of the authority argument (i.e. compliance with the Law). With this said, it should give some insights into the validity of recent law enforcement agencies' DPI practices.

A. The different types of packet inspections

In order for the data to be transmitted within and across the network, communication standards are needed. The TCP/IP[5] networking model was developed over thirty years ago to standardize

[2] As evidenced by Andreas Kuehn and Milton Mueller in "Profiling the Profilers: Deep Packet Inspection for Behavioral Advertising in Europe and the United States", 2012, accessed February 20, 2014, http://ssrn.com/abstract=2014181.
[3] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJ L 178, 17.7.2000, p. 1–16.
[4] Recital 42.
[5] TCP stands for Transmission Control Protocol and IP for Internet Protocol.

how network devices communicate in an interoperable fashion[6]. TCP/IP is composed of four layers – link, network, transport and application – plus the physical layer over which the model runs, each of which implements a subset of functions necessary for end-to-end data transmission. The *physical layer* defines the actual media over which the data are being transmitted; the *link layer* formats the packet so that it can be sent from its point of origin to its destination, or where necessary to the next router towards the destination; the *network layer* is responsible for the packet's addressing and routing; the *transport layer* organises the data transmission process in several sequential steps by segmenting data from upper levels and reassembling the data flow into smaller units, and (in the case of TCP) establishes a connection between the packets' sender(s) and recipient(s); the *application layer* interacts with the software applications that are making a data request.

The demarcation line between the IP packet header and the IP packet payload is a fundamental aspect of the definition of DPI. It derives from the TCP/IP model described above: the link, IP and transport layers each add a 'header' to a packet, whereas the application layer manages what is termed the 'payload' of a packet.[7] In practice, an application's data may be split over many IP packets when sent over the network. The original design of IP assumed that routers would scan only the IP packet header – that is, the delivery information, most commonly the IP destination field, relevant to moving the packet across the network[8]. The IP packet header contains basic routing information – in particular the source and destination IP address, which tells routers how to handle and forward the packet along to its destination.

The transport layer lies between the IP layer and the application layer, and thus a transport header exists between the IP packet header and the packet payload. The transport header indicates the source and destination applications at the communicating endpoints, e.g. a web browser and a web server, and these are identified by 'port numbers', with certain applications generally (but not always) using well-known port numbers, such as port 80 for unencrypted web (HTTP[9] protocol) traffic.

The combination of source and destination IP addresses and ports, together with the protocol used, e.g. TCP, forms a 'five tuple' or '5-tuple' that is commonly used in various networking contexts to identify specific application flows. Such information is often referred to as one form of 'metadata' for the traffic.

There are different perspectives on packet inspection. Strictly speaking, DPI systems allow the inspection of not only the metadata of the packets traveling across the network, but also the inspection of the sent content; that is why, deep packet inspection is often referred to as whole-packet inspection.[10] The payload or content of the packet[11] contains information about what application is sending the data, whether the packet's contents are themselves encrypted, and what the actual content of the packet is. Internet packets do not have only a single header and payload; instead, there is a packet header and payload at each layer of the multi-layered Internet architecture that can be found in each network-connected host.[12] Different views of those headers and layers are illustrated below in Figure 1, where Figure 1(a) shows the complete contents of an IP packet as available to a DPI system. DPI reveals not only which systems are

---

[6] Andrew S. Tanenbaum and David J. Wetherall, *Computer Networks*, 5th Edition, (US: Pearson, 2010).

[7] Alison Cooper, "Doing the DPI Dance: Assessing the Privacy Impact of Deep Packet Inspection", in *Privacy in America: Interdisciplinary Perspectives,* ed. William Aspray and Phillip Doty (Maryland: Scarecrow Press, 2011), 142.

[8] Ralf Bendrath and Milton Mueller, "The end of the net as we know it? Deep packet inspection and Internet governance", *New Media & Society* 13(7) (2011): 1147.

[9] HTTP stands for Hypertext Transfer Protocol.

[10] Chris Fuchs, "Societal Impacts of Deep Packet Inspection Internet Surveillance", *Information, Communication & Society* 16(8) (2013): 1342.

[11] Which should not be confused with the legal concept of communication content or correspondence.

[12] Klaus Mochalski and Hendrik, Schulze, "Deep Packet Inspection: Technology, Applications & Net Neutrality", White Paper, IPOQUE, 2009, accessed February 25, 2014, http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf. p. 4.

communicating, but also the operation or, in the case of a web request, the specific file being accessed.

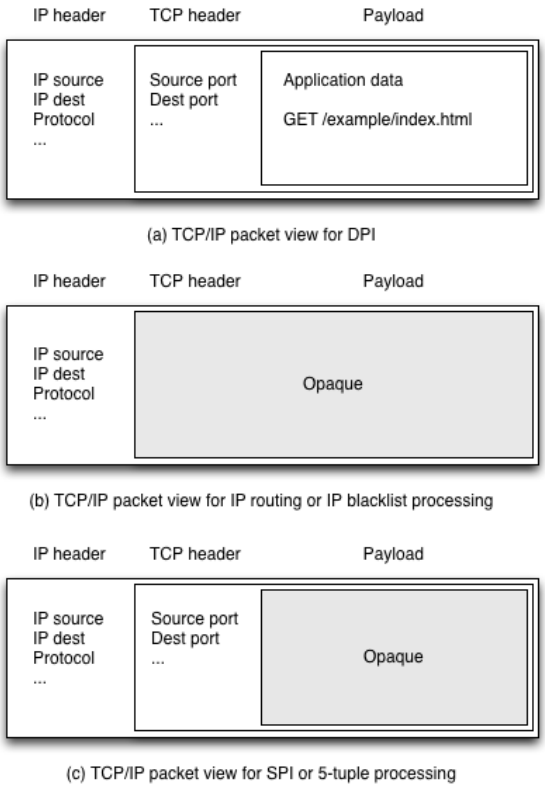

Figure 1: Different TCP/IP packet views

As aforementioned, an IP router, which needs to decide how to forward an IP packet towards its destination, generally only needs to make that decision based on the IP destination address in the packet. The rest of the packet, including the transport header and the payload, are opaque to the router, as illustrated in Figure 1(b).

In some cases a router may have Access Control Lists (ACLs) configured, to perform some packet filtering function, in which case it is common for the router to look at the transport header as well, to identify the port numbers in use, and then make a decision to filter based on some or all of the 5-tuple present. In such cases, the router's view is as per Figure 1(c), with only the application payload remaining opaque to the monitoring device.

There is an argument, because the inspection of the transport (e.g. TCP or UDP[13]) header is not in principle needed to route packets across the network and because the observed ports used gives some insights as to the nature of the activity of Internet users, that one could adopt Cooper's definition of DPI which reads as follow: "[d]eep packet inspection is the collection, observation, analysis, and/or storage of data related to an application that is found in Internet packets above OSI layer 3".[14] Or in the TCP/IP model, packet headers or content above the network layer.

With this said, depending on the TCP/IP layers that packet inspection technologies can analyse, there are three 'classes' of these technologies that are used in networking environments; shallow, medium and deep in the sense of whole packet inspection.[15] The TCP/IP model can be used to express the extent of information that inspection technologies can derive from packets; the

[13] UDP stands for User Datagram Protocol and is an alternative to the TCP.

[14] Cooper, "Doing the DPI Dance: Assessing the Privacy Impact of Deep Packet Inspection", 145.

[15] Thomas Porter, "The Perils of Deep Packet Inspection", Symantec, October 19, 2010, accessed February 28, 2014, http://www.symantec.com/connect/articles/perils-deep-packet-inspection.

closer such a technology comes to examining the application layer part of the payload, and the further it looks into the payload, the more information it can learn about the packet passing through the inspection device.[16]

Shallow Packet Inspection (SPI) examines the packet's IP and transport header information to decide whether to allow the packet to pass. It might make a decision to only allow traffic to port 80 or 443 (the well-known ports for plain or encrypted web traffic) to certain IP addresses. Or it might check the destination IP address against a blacklist (e.g. of known malware command and control servers); if the IP address is on the blacklist, the packet is not delivered. With SPI it is not possible to peer inside a packet's payload to survey the packet's content.[17] Thus SPI covers the cases illustrated in Figure 1(b) and (c). If a SPI system notes information about a packet, and uses that to influence decisions on future packets seen, it is known as a 'stateful packet inspection' system; an example is that such a system may let UDP traffic out, and only allow UDP traffic back in to its network that match the traffic sent out.

The second class of packet inspection technologies – Medium Packet Inspection (MPI) - involves the use of *application proxies*, devices that act as intermediaries between end-users' computers and Internet gateways, through which all the traffic passes. An example might be a web cache or proxy, used by an ISP or a site such as a university campus network. Application proxies examine packet headers and a small amount of payload against *parse-lists* for particular representations; every parse-list contains a set of representations. MPI devices decide whether a specific packet-type is permissible or not according to its data format type and its associated location on the Internet. Due to their ability to read the application commands located within the application layer as well the file formats in the presentation layer, MPI devices can prevent users from receiving specific types of files or prioritize specific files over others.[18]

Whereas MPI devices have very limited application awareness, whole packet inspection devices are designed to allow ISPs or the organisations using them to precisely identify the origin and – more importantly – the content of each packet that passes through their networks. Whole packet inspection devices can examine all the headers as well as the whole content of the messages due to their ability to look at every layer of the TCP/IP model.[19] Whole packet inspection technologies enable ISPs to gain greater control over every facet of their network operations.[20]

Consequently, because only MPI and whole packet inspection technologies reach the payload, others have decided not follow Cooper and exclude SPI from the definition of DPI.

The primary capability that underlies DPI is recognition, which can trigger two other capabilities – manipulation and notification.[21] A DPI system reaching the payload first creates a data structure to represent the incoming packets as network flows by collecting packets from the network interface cards, and then it searches for well-known patterns within the payload for each flow.[22] Based on the recognition of a regular pattern in the payload, the system can make decisions about how to handle the packet, which in turn allows networks to classify and control

---

[16] Chris Parsons, "Deep packet inspection in perspective: tracing its lineage and surveillance potentials", The New Transparency Surveillance and Social Sorting Working Paper, January 10, 2008, accessed March 2, 2014, http://www.christopher-parsons.com/Academic/WP_Deep_Packet_Inspection_Parsons_Jan_2009.pdf. p. 5.

[17] Angela Daly, "The Legality of Deep Packet Inspection", *International Journal of Communications Law & Policy*, No 14 (2010): 2.

[18] Parsons, "Deep packet inspection in perspective: tracing its lineage and surveillance potentials", 7.

[19] Chris Fuchs, "Implications of DPI Internet Surveillance for Society", The Privacy & Security Research Paper Series, PACT, Issue 1, 2013, accessed March 5, 2014, http://www.projectpact.eu/privacy-security-research-paper-series/%231_Privacy_and_Security_Research_Paper_Series.pdf. p.55; Office of the Privacy Commissioner of Canada, "Review of the Internet Traffic Management Practices of Internet Service Providers", February 18, 2009, accessed March 1, 2014, www.priv.gc.ca/information/research-recherche/sub/sub_crtc_090728_e.asp

[20] Cooper, "Doing the DPI Dance: Assessing the Privacy Impact of Deep Packet Inspection", 145.

[21] Milton Mueller, "DPI Technology from the standpoint of Internet governance studies: An introduction", accessed February 28, 2014, http://dpi.ischool.syr.edu/Technology_files/WhatisDPI-2.pdf. p.4.

[22] Rafael Antonello et al., "Deep packet inspection tools and techniques in commodity platforms: Challenges and trends", *Journal of Network and Computer Applications* 35(6) (2012): 1872.

traffic, application and subscribers.[23] To begin with, the recognition process relies on mechanisms that compare the packet payload to a set of strings, which represent predefined patterns called *regular expressions*. More precise information about where to look for such patterns is then provided by *signatures*, which help the identification process. Finally, *rule sets* provide DPI engines with more specific instructions, e.g. which signatures should be applied to which traffic between specific points. The recognition capability can be used to detect a variety of things, such as text strings, media content (specific instances of images, music or movies), URLs, viruses and other exploits, applications and protocols.[24]

A system with such inspection capability, where it is specifically designed to detect patterns indicating network attacks, malware or similar, is commonly referred to as an intrusion detection system (IDS). It is very common for large site networks, such as university networks, to use an IDS, to help protect its systems and its users.

As mentioned above, the second basic technical DPI capability is manipulation, which is dependent upon the recognition capability. Based on rule sets – instructions that make the network behave in a certain way – the manipulation capability enables a DPI appliance to actively intervene in a live traffic stream in order to modify or control it, e.g. regulate packet flow speed, block the movement of informational objects into the network, prioritise some protocol packets or users over others or even disconnect a session. Whereas the signatures used in the recognition process are supplied and maintained by DPI vendors, the rule sets for manipulating the content are defined by network operators.

For an IDS, if the system reacts in real-time to the patterns matched, it may act as an intrusion prevention system (IPS) by signalling a firewall system to block traffic to/from the 5-tuple observed as associated with the suspected attack or malware activity.

A less direct form of intervention also contingent upon recognition is the notification capability, which is used by DPI engines to generate statistical reports, issue alarms or notifications etc.[25]

Due to the above capabilities, DPI technology has been compared to a postal worker who opens all letters and packets, checks the content against databases of appropriate content, destroys letters or sends a copy to the police authorities when finding a match, and sends packages for its own mail service at a faster speed.[26]

Many of the functions provided by DPI technology have been available before; what differentiates DPI from other technologies are the following unique characteristics. First, in addition to inspecting the packet header, not only can DPI use any part of the packet for detection, but it also looks for patterns across multiple packets.[27] Another key feature of DPI is that, unlike several applications that scan digital content stored on servers or computers, DPI scans information in motion, not information at rest. The scanning of data packets takes place in real time.[28] What is more, DPI equipment allows network operators to make decisions that involve more than merely where to forward the packet; network operators monitor the content of data packets in real-time and make decisions about how to handle them.[29]

---

[23] Bendrath and Mueller, "The end of the net as we know it? Deep packet inspection and Internet governance", 1150.

[24] Mueller, "DPI Technology from the standpoint of Internet governance studies: An introduction", 8.

[25] *Ibid.*

[26] Bendrath and Mueller, "The end of the net as we know it? Deep packet inspection and Internet governance", 1152. This comparison is however misleading to the extent an automated filtering process only looks for specific types of information contained within communications and therefore does not always comprehend and is not always capable of remembering the whole content of these communications.

[27] Mochalski and Schulze, "Deep Packet Inspection: Technology, Applications & Net Neutrality", 6.

[28] See Nick S. Artan and Henry J. Chao, "Design and analysis of a multipacket signature detection system", *International Journal of Security and Networks* 2(1–2) (2007): 123.

[29] Chris Parsons, "Deep Packet Inspection and Its Predecessors", 2012, accessed February 28, 2014, http://www.christopher-parsons.com/Main/wp-content/uploads/2013/02/DPI-and-Its-Predecessors-3.5.pdf. p. 3.

It is useful to note here though that it is becoming increasingly challenging for DPI to be performed in real-time on high-speed Internet backbone networks, where speeds at the time of writing are commonly now 100Gbit/s. It is thus generally easier to perform DPI closer to the edge of a network, where the link speeds are slower. Or the ISP may 'pre-filter' traffic based on destination IP address, and re-route that traffic to a DPI system that only looks inside traffic to specific IP addresses that the ISP (or someone they are acting on behalf of) is interested in (which is how we believe the UK's Cleanfeed system operates, as discussed in the next section). Or alternatively it may be necessary to only sample a certain percentage of the network traffic.
We should also note here that effective DPI is only possible when the payload is plain text; where encryption is used the ISP would then need to be able to break that encryption in order to inspect the payload. Recently, both Facebook (due to security concerns over account hijacking) and Google Mail (post Snowden revelations) have made traffic to their systems encrypted by default. In cases where IPsec[30] is used, which may include virtual private networks (VPNs), other layer header information may also be unavailable to a 3rd party monitoring system, the specifics depending on whether end to end or tunnel mode IPsec is used.

B. Content regulation and DPI

Despite public outcry generated by the implementation of DPI technologies at the initiative of the industry to regulate online content (1), the legal scrutiny developed to assess the validity of these practices at the European level (2) and at the national level (3) has not proved to be very demanding. National judges in particular have denied any privacy implications.

1. Private experiments

In order to deal with illegal child sexual abuse content available on the Web, the UK has adopted an industry-led approach. Since 1996, the Internet Watch Foundation (IWF)– a private body funded by the Internet industry and the EU – has acted as a hotline receiving public complaints and, in case these complaints are grounded, forwarding them to the police as well as asking the UK-based hosting providers to have that material removed.[31]
In spite of the remarkable success of this approach, it was not effective when the illegal material was hosted abroad.[32] To address this problem, British Telecom (BT) developed a technical system, called Cleanfeed, aiming specifically at blocking access to child abuse images hosted outside of the UK jurisdiction. The stated purpose of Cleanfeed was to prevent Internet users from accessing, either accidentally or by design, illegal child abuse images.[33]
The Cleanfeed system was designed to be a low cost, but highly accurate, method of blocking unacceptable content; this filtering technology is a hybrid system, which combines the redirection of traffic (IP address re-routing) and DPI-based URL blocking, and operates as a two-stage mechanism to filter specific Internet traffic.[34] The first stage is based on the examination of the IP address and the destination port of the packets travelling across the network against the IWF database. In case the traffic is suspicious, then it is redirected to the second stage of filtering, which is implemented as web proxy that understands HTTP requests.

---

[30] IPsec stands for Internet Protocol Security. This protocol suite is used to secure IP communications and relies upon authentication and encryption techniques. See the IETF RFC at http://tools.ietf.org/html/rfc4301, accessed June 28, 2014.
[31] Internet Watch Foundation https://www.iwf.org.uk/.
[32] TJ McIntyre, "Child Abuse images and Cleanfeeds: Assessing Internet Blocking Systems", in *Research Handbook on Governance of the Internet,* ed. Ian Brown (UK: Edward Elgar Publishing Ltd., 2013), 302.
[33] Richard Clayton, "Failures in a Hybrid Content Blocking System", in *Privacy Enhancing Technologies 5th International Workshop Revised Selected Papers*, ed. George Danezis et al, Cavtat, Croatia, May/June 2005, 81.
[34] House of Commons Culture, Media and Sport Committee, "Harmful content on the Internet and in video games", Tenth Report of Session 2007–08 Volume II, accessed March 1, 2014, http://www.publications.parliament.uk/pa/cm200708/cmselect/cmcumeds/353/353ii.pdf. p.369.

When the request matches an item from the IWF blacklist containing URLs of child sexual abuse content, a *404 response* is returned; 404 response is a HTTP standard response code indicating that the server could not find what the client requested.[35] At the time of its implementation, the Cleanfeed technology was regarded as a substantial step forward over the two main schemes of filtering then in use; in contrast with the IP address blocking, the use of web proxies, which were as selective as necessary, prevented the danger of over-blocking, while it ensured that only web traffic – not other protocols – would be affected by avoiding the second existing scheme, DNS poisoning.[36]

Despite the fact that BT designed the Cleanfeed system in such a way as to be used only for the protection of its customers – not for prosecution purposes – by avoiding logging data on users,[37] its implementation has been described as "the first example of mass censorship on the Web attempted in a Western democracy".[38] What prompted public criticism was the power given to a private body to take censorship decisions for the UK Internet users by determining whether the content is potentially illegal, with limited procedural safeguards and no oversight.[39] An example of the implications that a filtering system such as Cleanfeed could have is the Wikipedia incident.[40] In December 2008, the URL of a Wikipedia article was added to the IWF list because of containing a pornographic image of a child, which was the cover image of a Scorpions album being legally sold since 1976. As a result, UK traffic for Wikipedia was redirected via the Cleanfeed servers; instead of blocking access to the specific URL of the offending image, access to the entire page of the band was blocked. After reviewing the situation, the IWF removed the listing four days later.[41]

The need for legislative basis for the adoption of any blocking system was the main point of criticism, especially given the difficulties in striking the right balance between fighting child pornography and maintaining the freedom of expression.[42] With this said, no ad hoc legislative framework has never been adopted. On the contrary as explained below, English courts have required Internet access providers to extend the scope of this technology and use it for blocking access to copyright infringing websites. Such an extension is naturally a concern, given the scope or creep of such filtering could be expanded further, in response to whichever lobbying groups come to the courts next to protest a given use of the Internet.

In 2008, a company named Phorm, whose aim was to help advertisers better target consumers by monitoring their web browsing habits, raised much ire from privacy campaigners. Phorm was in partnership with three of the UK's biggest ISPs – BT, Virgin Media and Talk Talk – which were planning to use the Phorm service, a patent-pending technology that delivered personalised content and advertising to ISP customers.[43] As it was revealed, BT had already carried out secret small-scale trials in 2006 and 2007, where, in both cases, the users were unaware of the tests and

---

[35] Clayton, "Failures in a Hybrid Content Blocking System", 82.

[36] *Ibid.* 92

[37] Malcolm Hutty, "Cleanfeed: the facts", LINX Public Affairs, 2004, accessed March 5, 2014, https://publicaffairs.linx.net/news/?p=154.

[38] Martin Bright, "BT puts block on child porn sites", *The Guardian*, June 6, 2004, accessed March 2, 2014, http://www.theguardian.com/technology/2004/jun/06/childrensservices.childprotection.

[39] Chris J. Davies, "The hidden censors of the Internet", *Wired*, May 20, 2009, accessed February 28, 2014, http://www.wired.co.uk/wired-magazine/archive/2009/05/features/the-hidden-censors-of-the-internet.aspx?page=all.

[40] Richard Clayton, "IWF, Wikipedia and the "Wayback Machine". UKNOF13, Sheffield, May 28, 2009, accessed March 2, 2014, http://www.uknof.org.uk/uknof13/Clayton-IWF.pdf.

[41] John Naughton, "Wikipedia censorship highlights a lingering sting in the tail", *The Guardian*, December 14, 2008, accessed March 1, 2014, http://www.theguardian.com/technology/2008/dec/14/wikipedia-censorship-scorpions-virgin-killer.

[42] Lilian Edwards, "Pornography, Censorship and the Internet", in *Law and the Internet,* ed. Lilian Edwards and Charlotte Waelde (Oxford: Hart Publishing, 2009), 76.

[43] Toby Stevens, "Phorm: a new dawn for web advertising?", *Computer Weekly*, April 22, 2008, accessed March 7, 2014, http://connection.ebscohost.com/c/editorials/32043271/phorm-new-dawn-web-advertising.

thus had not actively given their consent. Phorm Service deployed DPI-based advertising technique, which involved equipment installed in an ISP's network that intercepted all web traffic passing along every customer's broadband connection, and scanned through it for keywords that could be used to deliver targeted advertising – advertising that reflects customers' communication flows[44]. User's IP addresses were said not to be stored.

The main criticism of Phorm, as it was planned to be implemented in the UK, focused on the fact that it would have been an opt-out service, which meant that no prior consent would have been required for the users' data to be monitored.[45] Some even stated that even if users decided to opt out of the service, they would still continue to have their browsing histories stored by Phorm.[46] Fearing that such a technology could set a worrying precedent, that intercepting technologies would be perfectly acceptable for commercial reasons, many government officials questioned the legality of an opt-out programme; in April 2008, the Information Commissioner's Office stated that Phorm's system would only be legal under UK law as an opt-in service. The Phorm scandal eventually triggered the European Commission into launching an Infringement Proceeding against the UK, in April 2009, for failing to fully implement the data protection Directive and the ePrivacy Directive.[47]

A few months later, in an attempt to measure the level of music copyright on its network via peer-to-peer protocols, Virgin Media UK planned to deploy Detica CView technology on a trial basis beginning at the end of 2009, which would have involved monitoring 40 per cent of its customers without their knowledge or prior consent.[48] CView is a DPI product based on the same technology that powered the controversial Phorm's advertising system; it identifies peer-to-peer packets and then it looks at the actual content of those packets including application data in order to determine whether the copyrighted work exchanged is licensed or not, based on data provided by the record industry.[49] CView was designed to look for three types of file-sharing traffic - eDonkey, Gnutella and BitTorrent.[50] As the company's aim was to establish an 'index' of copyright infringements – not to keep records on individual customers – Virgin emphasized that data on the level of copyright infringement would be aggregated and anonymised.[51] Indeed, once CView identified an eDonkey, Gnutella or BitTorrent session, it would strip out the IP address of the user from each packet replacing it with a randomly-generated unique identifier and pulling out an 'acoustic fingerprint'. It would then send the processed material on to a central server to be matched against a database of acoustic fingerprints of copyright songs provided by record companies.[52] However, despite the fact that Virgin claimed that processed data would be anonymised, privacy campaigners protested against the implementation of such technology arguing that using that technology to identify those using torrents or blocking the content would

---

[44] Richard Wray, "Phorm: UK faces court for failing to enforce EU privacy laws", *The Guardian*, April 14, 2009, accessed March 7, 2014, http://www.theguardian.com/business/2009/apr/14/phorm-privacy-data-protection-eu.

[45] Andrew McSaty, "Profiling Phorm: an autopoietic approach to the audience-as-commodity", *Surveillance & Society* 8(3) (2011): 313.

[46] See e.g. Simon Heron, "Online privacy and browser security", *Network Security*, 6 (2009): 5.

[47] European Commission, "Telecoms: Commission launches case against UK over privacy and personal data protection", April 14, 2009, EC IP/09/570, accessed March 1, 2014, http://europa.eu/rapid/press-release_IP-09-570_en.htm.

[48] ISP Review, "Virgin Media UK Halt Broadband ISP Trial of CView DPI to Track Illegal File Sharing", October 10, 2010, accessed March 5, 2014, http://www.ispreview.co.uk/story/2010/10/01/virgin-media-uk-halt-broadband-isp-trial-of-cview-dpi-to-track-illegal-file-sharing.html.

[49] Christopher Williams, "Virgin Media to trial filesharing monitoring system", *The Register,* November 29, 2009, accessed March 5, 2014, http://www.theregister.co.uk/2009/11/26/virgin_media_detica/.

[50] Christopher Williams, "Spook firm readies Virgin Media filesharing probes", *The Register,* December 2009, accessed March 5, 2014, http://www.theregister.co.uk/2009/12/07/detica_visit/.

[51] ISP Review, "EC to Monitor DPI CView Trial on Virgin Media UK Broadband ISP Users", January 28, 2010, accessed March 5, 2014, http://www.ispreview.co.uk/story/2010/01/26/ec-to-monitor-dpi-cview-trial-on-virgin-media-uk-broadband-isp-users.html.

[52] Williams, "Spook firm readies Virgin Media filesharing probes".

only require "a slight tweak to the software".[53] Several events following the announcements of Virgin made the company reconsider the use of the CView system and put the trial on hold.[54] At this stage, it is worth noting that there are many perfectly legitimate uses of peer-to-peer applications such as BitTorrent, e.g. for sharing large research data sets, performing distributed backups, or, as used by Blizzard for its MMORPG World of Warcraft© to distribute game updates to its (currently estimated) 8,000,000 registered players. Thus it is 'dangerous' to block BitTorrent itself, rather an ISP would need to be sure the content were (or at least part of) a copyright-offending file. In some Member States it would then need to address the question whether the use of a copyrighted work could be justified on the ground of an exception, e.g. parody or pastiches[55].

By looking at how the legal framework has evolved it is however arguable that such a self-regulatory attempt to tame the infringing exchange of copyrighted works via peer-to-peer networks could easily survive legal scrutiny. Indeed on one hand the findings of the CJEU are ambiguous. On the other hand, national judges have on several occasions refused to identify any significant privacy implications in relation to the deployment of DPI practices.

2. The European framework

In Sabam[56], the claimant Sabam, a management company representing authors, composers and editors of musical works had found that Internet users using the services of Scarlet (an Internet access provider) were exchanging copyrighted works belonging to Sabam's catalogue without its authorisation, through the means of peer-to-peer networks. Sabam among other things asked the Brussels Tribunal of first instance to order Scarlet to block or make it impossible for its customers to upload or download files containing copyrighted works via peer-to-peer networks without prior authorisation.

While the Tribunal of first instance granted the request, the Court of Appeal referred the case to the CJEU asking in particular whether a court could "order an [ISP] to install, for all its customers, in abstracto and as a preventive measure, exclusively at the cost of that ISP and for an unlimited period, a system for filtering all electronic communications, both incoming and outgoing, passing via its services, in particular those involving the use of peer-to-peer software, in order to identify on its network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold rights, and subsequently to block the transfer of such files, either at the point at which they are requested or at which they are sent".

To rephrase the question by identifying the technology at stake, the national court of Appeal was asking whether a court could order an ISP to implement DPI techniques such as the Audible Magic's CopySense system to block the exchange of copyrighted works. "Audible Magic's CopySense™, a network appliance product, examines network traffic at the content layer —– that is, it analyzes the actual file transferred in an application-layer transaction. In other words it is an example of whole packet inspection. In order to determine whether the content is a copyrighted song, CopySense treats the content as audio and analyzes its acoustic properties. It examines only a small portion of the content, extracting an "acoustic fingerprint.""[57]

---

[53] Chris Nickson, "Virgin Media to begin CView trials", *Techradar*, December 10, 2009, accessed March 6, 2014, http://www.techradar.com/news/internet/virgin-media-to-begin-cview-trials-657287#null.

[54] ISP Review, "Virgin Media UK Halt Broadband ISP Trial of CView DPI to Track Illegal File Sharing".

[55] See e.g. art. L.122-5 of the French Code of Intellectual Property and more generally art. 5 of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Official Journal L 167, 22/06/2001 p. 10 - 19.

[56] CJEU case C-70/100 Scarlet v Sabam of 24 November 2011 [2012] E.C.D.R. 4 (Sabam).

[57] Chris Palmer, "Audible Magic — No Silver Bullet for P2P Infringement", *Staff Technologist*, July 12, 2004, accessed February 25, 2014, http://w2.eff.org/share/audible_magic.html. See also Audible Magic's White Paper, "Managing Peer-to-Peer Traffic with the CopySense™ Network Appliance", July 23, 2004, accessed February 25, 2014,

The answer given by the CJEU remains ambiguous[58]. Truly the court attempts to assess the validity of the contentious DPI practice from different angles (Article 15 of the e-commerce Directive, freedom to conduct one's business, the principle of proportionality, the right to the protection of personal data and freedom of expression). The CJEU thus holds that "active observation of all electronic communications conducted on the network of the ISP" [59] encompassing all information to be transmitted and targeting all the ISP's subscribers amounts to a general obligation to monitor within the meaning of Article 15 of the e-commerce Directive. Yet Article 15 prohibits the imposition of such obligations upon intermediary providers such as Internet access providers. While the CJEU's understanding of how the technology is supposed to function seems to be approximate in as much as not all packets are actively observed (only those targeted at a specific IP address or a specific port number), it does seem that what is really problematic to the eyes of the CJEU is the observation of packet payload and in particular application data.

In relation to the right to the protection of personal data it observes that the order requested would "involve a systematic analysis of all content and the collection and identification of users IP addresses from which unlawful content on the network is sent. Those addresses are protected personal data because they allow those users to be identified" [60]. Once again the CJEU's understanding of how the technology is supposed to function appears approximate: not all packet payloads are inspected, only those transmitted through the means of suspicious ports, and the routing of packets implies per se the processing of IP addresses. As a result the collection of IP addresses cannot be the real source of concern. What remains an issue though is the processing of packet payload including application data which is followed by a digital sanction (behaviour modification): the inability to access or exchange copyrighted works.

Yet the CJEU does not say expressly that the DPI practice at stake violates the principle of confidentiality of communications and does not mention Article 15 of the data protection Directive which could seem relevant in such a scenario. Indeed Article 15 provides that "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc".

Besides, by focusing upon the prohibition of the imposition of a general obligation to monitor as protected by Article 15 of the e-commerce Directive and the freedom to conduct one's business (the judgment starts with these considerations) the CJEU could be saying that if DPI practices are adopted voluntarily they become more legitimate and could be held legally valid.

In the Netlog case, [61] the reasoning of the CJEU is less problematic in as much as the infrastructure supplied by the service provided is different. In this case a social networking website[62] had been asked to inspect the data stored on its servers in order to block the exchange of infringing content. As a result, most packet payloads get to be inspected. However, at the same time, it is arguable that in several cases the service provider cannot be bound by any confidential obligation. Hence the different wording used by the CJEU which this time states that the filtering system "would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users. The

---

https://www.audiblemagic.com/2004/06/23/audible-magics-copysense-network-appliance-manages-p2p-traffic-at-college-preparatory-school/.

[58] Sophie Stalla-Bourdillon, "Online monitoring, filtering, blocking ….What is the difference? Where to draw the line?", *Computer Law & Security Review: The International Journal of Technology Law and Practice* 29 (6) (2013): 702-712.

[59] Sabam at [39].

[60] Sabam at [51].

[61] CJEU case C-360/10 Sabam v Netlog of 16 February 2012 [2012] 2 C.M.L.R. 18 (Netlog).

[62] At [16] the CJEU states that "Netlog runs an online social networking platform where every person who registers acquires a personal space known as a 'profile' which the user can complete himself and which becomes available globally".

information connected with those profiles is protected personal data because, in principle, it allows those users to be identified". It is not clear however whether it is the retention of personal data that is the real concern or the collection of personal data. In addition, the fact that the hosting provider had been asked to modify behaviour is not expressly identified as a concern by the CJEU. Moreover, it is arguable once again that if such filtering practices are adopted voluntarily they could be deemed as legally valid.
Unsurprisingly, in the recent case UPC Telekabel in which the CJEU had to assess the validity of a generic injunction requiring an Internet access provider to block access to an infringing website the right to private life is not even mentioned.[63] Besides, it is for the Internet intermediary to select the appropriate technology to implement the generic order issued by the judge.[64]

3. National interpretations

The case EMI Records (Ireland) Ltd and Others v UPC Communications Ireland Ltd[65] came before Charleton J. before the issuance of the Sabam and Netlog decisions.
In this case copyright owners claimed for an injunction against an Irish Internet access provider (UPC) ordering the service provider to prevent the commission of copyright infringement through the means of peer-to-peer networks. The claimants had indeed been using detection software to identify the IP addresses of alleged infringers. They thus wanted UPC to collaborate with them and implement a graduate response system implying the warning of subscribers and eventually the termination of the service. UPC had refused to do so and the claimants were therefore asking the Irish judge of first instance to make UPC contribute to the fight against illegal file-sharing by e.g. ordering the implementation of a graduated response system or the implementation of filtering technologies amounting to the blocking of illegal exchanges of copyrighted works and thereby the implementation of whole packet inspection technologies.
Although s.40(4) of the Irish Copyright and Related Rights Act 2000 was very limited in scope and did not allow a judge to order an Internet access provider to implement a graduated response system or block illegal exchanges of copyrighted work[66], Charleton J. was of the view that such orders do not contravene the prohibition of the imposition of a general monitoring obligation upon mere conduits under Article 15 of the e-commerce Directive. Here are his words: "[d]eep packet inspection, as described in this judgment is not the seeking of information which is in the course of transmission. Instead, it identifies the nature of transmissions, whether encrypted or otherwise, by reference to the ports which they use, and the protocol employed, so as to identify peer-to-peer communication. UPC does this already for legitimate commercial purposes related to the management of transmissions. If it suited, they could also easily identify the file # of copyright works and block them or divert the search in aid of theft to a legal site. This is not a general search for information. It is simple use of deep packet inspection technology in aid of proper transmission".[67] In other words according to Charleton J. the systematic inspection of application data comprising the hash file of copyrighted works does not amount to general monitoring, which seems contrary to the ruling of the CJEU in the Sabam case.
Second, according to the Irish Judge ordering Internet access providers to implement graduated response systems or blocking technologies does not have any significant privacy implications. His position is quite radical: "I am of the view that there are no privacy or data protection implications to detecting unauthorised downloads of copyright material using peer-to-peer

[63] CJEU case C-314/11 UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH of 27 March 2014 (UPC Telekabel) at [47].
[64] UPC Telekabel at [53].
[65] [2010] IEHC 377 (EMI Records).
[66] A subsequent legislative amendment has however changed the state of the law. Such injunctions can now be granted. See the European Union (Copyright and Related Rights) Regulations 2012. The statutory instrument amends s.40 and s.205 of the Copyright and Related Rights Act 2000.
[67] EMI Records at [107].

technology"[68]. To support his view Charleton J. states that when a graduated response system is implemented the detection process is anonymous (only IP addresses are identified[69]) and the files transmitted are publicly made available[70]. As a result "deep packet inspection for the purposes of detecting and diverting or disenabling [peer-to-peer] transmissions" has no privacy or data protection repercussion. He had indeed noted in relation to DPI techniques that even if they reach the payload and application data there cannot be a violation of a privacy interest since only numbers (comprising the hash file) are read.[71] Besides, even if IP addresses can be combined to hash files corresponding to protected works, there are no privacy issue involved since it is not possible to identify the individual behind the IP address[72]. Charleton J. did however agree that "[t]his changes the passive transmission of internet service provider customer's data into intervention"[73].

In relation to the implementation of the CopySense technology by US universities the Irish judge went in the same direction and stated that the system in place does not look at content and therefore there is no privacy concern[74].

Such a view is problematic for several reasons. First because it does undermine the principle of confidentiality of communications (looking at the content of communications to determine whether they are worth of legal protection is undermining the very protection of these communications as provided in particular by Article 5 of the e-privacy Directive), the prohibition of the systematic monitoring of communication data as a tool of mass surveillance (to be found in Article 5 of the e-privacy Directive as well), the very definition of personal data (IP addresses are personal data when individuals are identifiable through the means of these data and Internet access providers do have the means to identify individuals with IP addresses as implied by the Sabam decision[75]), and the prohibition of automated individual decisions having legal effects under Article 15 of the data protection Directive (individuals are prevented from communicating and accessing content through the means of a pure automated process).

In EMI Records (Ireland) Ltd and others v The Data Protection Commissioner[76] decided in June after Sabam and Netlog, Charleton J. maintained his position: "[a]n activity of swarm participation for peer-to-peer downloading does not legitimately carry the expectation of privacy"[77]. Peer-to-peer communications are for the judge open communications. This is true despite the contrary view of the Irish Data Protection Commissioner who had disavowed the contracts entered by Eircom with its subscribers to implement a graduated response system in order to reduce the amount of illegal file sharing. Although referring to the Sabam and Netlog cases the Irish judge does not attempt to apply the European framework to the facts at hand. He simply refers to its implementation in the English case Twentieth Century Fox Film Corp v British Telecommunications Plc (Newzbin2) [78] and its progeny.[79]

In March 2010, the English High Court had granted an injunction against the Usenet indexing company Newzbin, which enabled users to exchange copyright infringing material.[80] Although

---

[68] EMI Records at [68].
[69] EMI Records at [68].
[70] EMI Records at [70].
[71] EMI Records at [38].
[72] EMI Records at [38].
[73] EMI Records at [39].
[74] EMI Records at [47].
[75] See Recital 26 of the data protection Directive.
[76] EMI Records (Ireland) Ltd and others v The Data Protection Commissioner [2012] IEHC 264 (EMI Records 2). The Irish Supreme Court in EMI Records (Ireland) Ltd & ors v The Data Protection Commissioner [2013] IESC 34 dismissed the appeal of the Data Protection Commissioner.
[77] EMI Records 2 At [7.2].
[78] [2011] EWHC 1981 (Ch).
[79] See e.g. Dramatico Entertainment Ltd v British Sky Broadcasting Ltd [2012] EWHC 268 (Ch), [2012] 3 C.M.L.R. 15; Golden Eye (International) Ltd v Telefónica UK Ltd [2012] EWHC 723 (Ch).
[80] Twentieth Century Fox Film Corp v Newzbin Ltd [2010] EWHC 608 (Ch).

the company claimed that it did no more than a search engine such as Google and should not be liable for its users' actions, while it also had a notice-and-take-down policy,[81] the Court ruled that Newzbin was liable for encouraging the downloading of works protected by copyright due to its knowledge of the infringements and its editorial involvement in making the infringement easier which amounted to both direct infringement and joint liability.[82]
The injunction effectively led to the closure of Newzbin, but an identical website, called Newzbin2, was subsequently opened using servers located in Sweden. Unable to target the website directly as that would have been beyond the jurisdiction of the UK, the same film studios that had successfully sued the Newzbin website, commenced proceedings to force the UK Internet access provider, BT, to block access to the website based on s 97A of the Copyright, Design and Patents Act of 1988. Arnold J. ultimately granted an injunction requiring BT to employ its blocking technology, Cleanfeed – originally designed to prevent access to websites or webpages featuring child sexual abuse – to block access to Newzbin2.
Cleanfeed could be seen as an example of whole packet inspection in as much as it targets URLs. The Court described Cleanfeed as a two-stage system of IP address re-routing, which entails the ISP using a proxy server inspecting the application data of packets containing the IP address of the infringing website, and eventually blocking the user's connection to the URL of the infringing website as defined in the network management systems access control lists[83].
Arnold J. stated that such an injunction was not equivalent to a general monitoring obligation within the meaning of Article 15 of the e-Commerce Directive and had no significant privacy or data protection implications because in this case BT was merely required to block access to Newzbin2 without any detailed inspection of any customer data despite the facts that, first, all BT's subscribers were subject to the re-routing of their packets to the proxy server each time the IP address of the infringing website was recognised in the IP header and, second, application data (URL) of those re-routed packets were inspected. To repeat Arnold J. words, the order sought required "simply to block (or at least impede) access to the Newzbin2 website by automated means that do not involve detailed inspection of the data of any of BT's subscribers".[84] Furthermore, the implementation of the order was not considered to be costly for the service provider since it had already set up the technology for other purposes.

To sum up, at the European level, it does seem that only the systematic inspection of the content of all communications transmitted over a public or private network is problematic either because it is contrary to Article 15 of the e-commerce Directive or because it has privacy or data protection implications[85]. However, it is arguable whether DPI technologies such as Cleanfeed or even CopySense amount to an inspection of the content of all communications for only the payload of suspicious communications is actually read when Internet service providers implement these technologies even though all subscribers are the targets of these measures. Besides, looking at national decisions, it does appear that judges have not be willing to find that DPI practices amount to the inspection of the content of communications even if the payload of packets is inspected either to identify the URL of the websites to be reached or hash files corresponding to copyrighted works.
But what does data protection law really say? Truly data protection law was not primarily meant to set appropriate limit to the deployment of surveillance technologies despite the little relevance of the distinction between content data and traffic data. It is however arguable that a series of provisions has been overlooked by judges essentially concerned about copyright piracy.

[81] Twentieth Century Fox Film Corp at [54].
[82] Twentieth Century Fox Film Corp at [126].
[83] Newzbin2 at [70] to [74].
[84] Newzbin2 at [162].
[85] The upshots of these decisions is even narrower in the sense the CJEU simply held that it is not possible to impose upon intermediaries a duty to implement these technologies for blocking purposes.

C. Data protection and DPI

At first glance, data protection law seems to legitimize the processing of personal data through the means of DPI techniques in several circumstances (1). With this said, this maybe reflects a partial overview and restrictive interpretation of data protection law (2).

1. The Lawful processing of personal data through the means of DPI

The data protection Directive[86] still remains the general legislative instrument governing the processing of personal data offline and online within the European Union. But when providers of publicly available electronic communications services or public electronic communications networks[87] are responsible for the processing, the data protection Directive has to be combined with another instrument adopted to take into account the specificities of the sector: the e-privacy Directive. [88] Said otherwise, the e-privacy Directive does not displace the data protection Directive. As explained in recital 10 "Directive 95/46/EC applies …to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals". To be more precise under Article 1(2) of the e-privacy Directive "[t]he provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1"[89].

Adopted to facilitate the free flow of personal data between Member states while protecting individuals, the drafters of the data protection Directive have included in the instrument a "generous" list of legitimizing ends. In particular under Article 7 of the Directive, the processing becomes legitimate if it is necessary for the purposes of the legitimate interests pursued by the data controller. Officially however the legitimate interests pursued by the data controller have to be balanced with those of the data subjects.

The e-privacy Directive expressly identifies several types of legitimate interest. Notably processing for the purposes of marketing electronic communications services or for the provision of value added services require prior consent from data subjects.[90]

Providers of publicly available electronic communications services or public electronic communications networks can process traffic data for the purposes of subscriber billing and interconnection payments under Article 6(2) without prior consent.[91] The same seems to hold true for fraud detection and traffic management as stated by Article 6(5)[92]. Nevertheless, only

---

[86] 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 Official Journal L 281 , 23/11/1995 p. 31 – 50.

[87] Article 3.

[88] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37 - 47 amended two times by Directive 2006/24/EC of the European Parliament and the of the Council of 15 March 2006 and Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

[89] The Article 29 Data Protection Working Party is of the view that if the processing is not allowed by the e-privacy Directive it cannot be allowed by data protection Directive. See Opinion 05/2014 on Anonymisation Techniques adopted on 10 April 2014, p. 8 (Anonymisation Techniques).

[90] Article 6(3).

[91] "Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may be lawfully challenged or payment pursued".

[92] The UK transposition however seems to be more restrictive in as much as it requires consent for both purposes. See The Privacy and Electronic Communications (EC Directive) Regulations 2003, s.8(3). By way of comparison the French transposition allows ISPs to process traffic data for security purposes without requiring prior consent under art. L34-1 of the French Postal and Electronic Communications Code (PECC). Nothing is said about traffic management purposes.

persons acting under the authority of these providers can process personal data for these purposes.

In this line, DPI has become an essential tool for network operators in their effort to obtain an in-depth knowledge of the underlying traffic composition and dynamics and thus be able to intervene in the management of that traffic. Specific applications can be passive aiming solely at giving the operator greater visibility, which is crucial for investment or pricing decisions, capacity planning etc.[93] When active elements are added to passive applications, DPI can contribute to bandwidth regulation or congestion response; DPI enables operators to discriminate among different types of traffic in order to provide satisfactory quality of service, or to throttle down excessive traffic.[94] When the recognition capability of DPI technology is combined with the manipulation capability, ISPs can prioritise (or de-prioritise) specific protocols, services or users. This market opportunity created by deeper and more granular traffic inspection allows ISPs to differentiate the online experience of individual users not only by bandwidth tiers, but on application and content bases as well; ISPs may apply different charging policies, traffic shaping, or offer quality of service guarantees to selected users or applications.[95] Historically, ISPs have generally only implemented traffic engineering or quality of service mechanisms, designed to give certain sites or applications better treatment than others, using IP addresses or the '5-tuple' (mentioned previously) of src/dst IP/port and protocol (e.g. TCP or UDP). However it is now more common for DPI to be used to identify specific application types (since several applications can use the same port) and thereby do load balancing or preform other functions to avoid congestion and eventually redirect the traffic in a different way around the network[96]. In this case no storing of data takes place, contrary to what happens with an IDS. DPI has been described as "a potentially disruptive technology"[97] as DPI used by ISPs can result in a violation of longstanding standards, such as net neutrality, and create a tiered Internet, which disadvantages certain users and application types, and is controlled by large companies.[98]

Recital 39 of the proposed general data protection Regulation also recognises the legitimising effect of insuring network security, which arguably is already encompassed by Article 7 of the data protection Directive. Recital 39 states that "[t]he processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams, - CERTs, Computer Security Incident Response Teams, - CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller". Some examples are given and concern mainly the prevention of criminal activities: the foregoing could "include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems".

Network security was in fact the earliest driver of the development of DPI technology; DPI can protect the network from attacks by monitoring, identifying and throttling traffic at all layers of

---

[93] Mueller, "DPI Technology from the standpoint of Internet governance studies: An introduction", 7.

[94] Peter Renals and Gareth Jacoby, "Blocking Skype through deep packet inspection" (paper presented at 42nd International Conference on System Sciences, Hawaii, 5–8 January, 2009).

[95] Antonello et al., "Deep packet inspection tools and techniques in commodity platforms: Challenges and trends", 1870.

[96] See Radisys' DPI software framework at http://www.radisys.com/products/atca/packet-processing/dpi-software-framework/, accessed June 28, 2014.

[97] Bendrath and Mueller, "The end of the net as we know it? Deep packet inspection and Internet governance", 1157.

[98] Fuchs, "Implications of DPI Internet Surveillance for Society", p.6.

the TCP/IP model.[99] DPI technology was first developed for intrusion detection and intrusion prevention systems. By combining malware recognition capabilities with packet capture and analysis techniques, DPI engines allow network operators "to detect and intercept recognised forms of threats before they reach their customers, such as keystroke loggers, bot infections, abnormal quantities of mail, command and control instructions from bot herders, or communications to servers known to be associated with botnets".[100] Not only are DPI engines able to identify threats but they can also respond to the detected threats by implementing measures to prevent the attack from succeeding, usually by terminating connections.[101] More specifically, DPI technology allows a security application to peer deep into the content of a data stream; certain patterns or signatures need to be found in the packet data in order for DPI to detect an attack on the network or other malicious behaviour. Reports are created for malware detection purposes and contain entries such as IPs, ports and the specific application commands. The e-privacy Directive combined with the data protection Directive therefore opens the door to a large amount of processing including processing for the purposes of ensuring traffic management and/or network security. The principle to be found in Article 6 of the e-privacy Directive mandating the erasing or making anonymous of traffic when they are no longer needed for the purpose of the transmission of a communication appears to be illusory to some extent.

With this said, an obstacle to the deployment of DPI practices could derive from Article 8 of the data protection Directive which prohibits the processing of sensitive data in the following terms: "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life". It is however possible to process such data if the data subject has given his explicit consent unless the Member state whose law is applicable does not recognise the legitimizing effect of the explicit consent of the data subject in these circumstances. It is true that collecting the content of communications or browsed information is likely to reveal sensitive data. However not all browsed information reveal sensitive data. In addition it could be argued that only the collection of the text of webpages could be prevented and not data relating to its format, location… which would leave a significant amount of data available for processing. Above all, the comparison between the packet payload and a set of strings for the purposes of detecting malware does not always reveal any sensitive data[102].

Another obstacle could be found in Article 5 of the e-privacy Directive recalling the importance of the right to the protection of one's correspondences in the information society[103].

Article 5 of the e-privacy Directive provides that "[m]ember States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of

---

[99] Network Strategy Partners, "Next Generation Deep Packet Inspection: An Overview of Requirements and Applications", March 2007, accessed February 25, 2014, http://0299d3f.netsolhost.com/NewPages/DPI.pdf. p.9.

[100] Mueller, "DPI Technology from the standpoint of Internet governance studies: An introduction", 7.

[101] Ioannis Sourdis, "Designs and algorithms for packet and content inspection" (PhD diss., Technische Universiteit Delft, 2007), accessed March 2, 2014, http://www.cse.chalmers.se/~sourdis/sourdis_phdthesis.pdf. p.42.

[102] This might be the case though when legitimate websites are hacked, the attacker puts malware on the site, and a visitor unknowingly then downloads the malware and gets infected. This is known as drive-by download.

[103] Truly, after the adoption of Directive 2009/36/EC[103] the processing of content data which implies the storing of information, or the gaining of access to information already stored in the terminal equipment of a subscriber or user (i.e. by using cookies) can only be done after having obtained the consent of the user or subscriber. But strictly speaking this only relates to information stored on the terminal of Internet users and not to information in transit or stored on service providers' servers. See Directive 2009/136/EC Of The European Parliament And Of The Council Of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation(EC)No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L337, 18.12.2009, p.11 - 36.

interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1)".
It is not sure however whether such an Article has been taken very seriously by all stakeholders.
It is sometimes assumed that DPI does not amount to interception. Under English law and s.2(2) of the Regulation of Investigatory Powers Act 2000 (RIPA) the "mere" monitoring of transmissions made by means of the system amounts to an interception as long as it has the effect of making "some or all of the contents of the communication available". If the inspection stops at the application header, strictly speaking content data have not been made available.
One difficulty lies down with URLs. The Code of Practice for the Acquisition and Disclosure of Communications Data (2003) provides that the part before the first slash in a website address is communications data, and what comes after the first slash is content; therefore, full URLs are regarded as content subject to a warrant.[104]
One could also argue that even if DPI technically amounts to an interception, it is ultimately a lawful interception since it is covered by s.3 of RIPA ("it takes place for purposes connected with the provision or operation of that service or with the enforcement, in relation to that service, of any enactment relating to the use of postal services or telecommunications services").
Another way of bypassing the prohibition of the interception of communications would be to draw a distinction between public and private networks as Charleton J. did in the aforementioned decisions and argue that there cannot be any interception when communications are transmitted over public networks.
Moreover, Article 15(1) of the e-privacy Directive refers to Article 13 of the data protection Directive and therefore implies that exceptions to Article 5 can be carved out for the protection of rights and freedoms of others. The principle of the confidentiality of communications is thus limited per definition and one could try to argue that at least for the purposes of safeguarding the security of the network ISPs should be allowed to implement DPI practices and inspect the network and transport layers as well as the application layer.
What is more, Article 4 of the e-privacy Directive[105] states that "the provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented". One could thus try to argue that DPI techniques should fall within the category of appropriate technical measures adopted to safeguard the security of the services provided.[106]

---

[104] Home Office, "The Code of Practice for the Acquisition and Disclosure of Communications Data", (pursuant to section 71 of the Regulation of Investigatory Powers Act 2000), 2003, accessed March 2, 2014, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97961/code-of-practice-acquisition.pdf. p.15-16("traffic data stops at the apparatus within which files or programs are stored, so that traffic data may identify a server or domain name (web site) but not a web page)". See also Draft Communications Data Bill Joint Committee - First Report, December 11, 2012, accessed March 2, 2014, http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/7902.htm, [77].

[105] See also Article 13a of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services ("Framework Directive") OJ L 108, 24/04/2002, p. 33–50.

[106] Most Internet and online service providers will, if the proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union is adopted, have in fact an obligation to take appropriate technical and organisational measures to manage the risk posed to the security of the networks and information systems which they control and use in their operations, to the exception of micro, small and medium-sized enterprises and thereby could be seen as being imposed an obligation to use mass surveillance techniques for the purpose of ensuring network security. At the same time, it is not clear whether control over preventive forms of processing undertaken for guaranteeing the security of networks will ever take place. National competent authorities on the security of network and information systems to be set up under Article 6 of the proposed Directive have for

Going further, data retention obligations depending upon their scope could be seen as simply trumping Article 5 of the e-privacy Directive. It is true that the data retention Directive has recently been held invalid by the CJEU[107]. However it is not sure whether such declaration will have radical consequences upon national transpositions[108] since what is at the core of the CJEU's decision is the impossibility to justify the interference with the right to private life and the right to the protection of personal data and in particular the absence or the non-harmonisation of safeguards in relation to access to the data to be retained and their eventual destruction[109]. Yet these safeguards or some of them could be found at the national level. It is thus worth recalling the Directive's very content. The data protection Directive could be read as imposing upon providers of publicly available services or public electronic communications networks an obligation to retain data obtained from the TCP/IP layers beyond the network layer and including the transport headers and payload. Indeed under Article 5 of the data retention Directive should be retained in particular "data necessary to identify the type of communication" including the internet service used, which could imply investigating the TCP or UDP header and the application header as well; data necessary to identify the destination of a communication including "the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication" which could imply investigating the application header[110]. In this sense traffic data should not be considered too quickly as a synonym to metadata since it comprises elements of the payload.
Article 5(2) did specify that "no data revealing the content of the communication may be retained pursuant to this Directive" which would mean that for the purposes of the data retention Directive content data only equated application data or certain types of application data such as the content of webmail messages.[111]

---

their main job to receive notifications of security incidents. They are thus supposed to intervene once the security threat has become looming (i.e. a risk) or real. See Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union – COM(2013) 48 final.

[107] CJEU Joined cases C-393/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marin and Natural Resources et al and Kärntner Landesregierung, Micheal Seitlinger, Christof Tschohl and others of 8 April 2014 (Digital Rights Ireland).

[108] With this said, in the UK at least the national transposition should be considered ultra vires since the Data Retention (EC Directive) Regulations 2009 is a type of secondary legislation adopted pursuant to section 2(2) of the European Communities Act 1972, allowing government ministers to introduce laws for the sole purpose of implementing EU Directives. In other Member States the application of the principle of subsidiarity might have the consequence of making national transposition legitimately stand on their own.

[109] The CJEU undertakes a strict scrutiny of the legislation. It observes that the data protection Directive covers "in a general manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being in the light of the objective of fighting against serious crime". It is thus a measure of mass surveillance (the persons concerned do not have to present a link, direct or indirect with serious crime) , the retention is not meant to be limited to certain time periods or geographical zones in order to establish a link with a specific threat to public security, no limitations are set for the access of the competent national authorities to the data and subsequent possible uses, no oversight mechanisms are established, the retention period is not strictly calibrated to the gravity of the threat to be prevented. In addition as regards Article 8 of the European Charter, the CJEU also notes that there is no distinction between different types of data in relation to their degree of sensitivity, there is no guarantee that the service providers at issue will implement a high level of protection and security to retain the data, that they will retain the data within the European Union, and, that the data will be destroyed at the end of the data retention period. Digital Rights Ireland, [34]ff. Besides, despite his conclusions in relation to the incompatibility of the data retention Directive with the Charter of Fundamental Rights of the European Union, the Advocate General does not seem to condemn all data retention obligations. Advocate General's Opinion in Joined Cases C-293/12 Digital Rights Ireland and C-594/12 Seitlinger and Others. Court of Justice of the European Union Press Release No 157/13. Luxembourg, 12 December 2013.

[110] It is important to note here that it is not practical for an ISP to keep all data flowing through it. It is far more practical to store only interesting traffic, such as that flagged by an IDS. What an IPS often does though is to store network flow information (the 5-tuple and a duration) to determine which IP/port spoke to which IP/port, for how long, with how much data, etc.

[111] Such an interpretation would echo that of English and Irish national judges.

One way of limiting the scope of the data retention Directive however is to interpret restrictively Article 3 which provides that only data generated or processed by providers of publicly available electronic communications services or of a public communications network could be retained, which should mean that if service providers do not take the initiative or do not need to look at the data relating to the recipient of the communication or the service used for examples for businesses purposes they could not be asked to retain these data.
But what if service providers such as Internet access providers are ordered to use DPI techniques to block access to some parts of the web? Shall the data inspected to this end also be retained? The answer should be negative to the extent the measure is primarily aimed at sanctioning unlawful websites and not the users accessing these websites themselves.

Even if traffic management and network security are legitimizing ends per se, which therefore implies that service providers do not need to obtain data subjects' consent when they are processing personal data for these purposes, these providers have to abide by the data quality principles such as the principle of finality (Article 6(b) of the data protection Directive) and the principle of data minimisation (Article 6(c) of the data protection Directive). As a result this would mean that the data processed cannot be used for other purposes and for example for building profiles of Internet users. However it is arguable whether the principles of finality and data minimisations are sufficient to protect the interests of ISPs' subscribers. Furthermore, those principles lose their strength when service providers are subject to extensive data retention obligations. In the end, it is likely that they are not enough to draw a foreseeable line between legitimate DPI practices and illegitimate DPI practices. Hence the necessity to go back to Article 8 of the ECHR and/or Article 7 of the European Charter, to gauge DPI practices and limit the number of cases in which personal data are retained by ISPs.

2. The confinement of the processing of personal data through the means of DPI

Even though Article 7 of the data protection Directive provides for a generous list of legitimizing ends, it does add that even if the processing of personal data pursues a legitimate interest of the data controller or third parties it can become unlawful if it seriously impairs the fundamental rights and freedoms of data subjects such as the right to private life.
Under the case law of the European Court of Human Rights (ECtHR) it is clear that both the interception of the content of communications and the 'mere' monitoring of traffic data for surveillance purposes does amount to a prima facie interference with the right to the protection of one's private life. In Copland v United Kingdom,[112] the applicant's telephone, email and Internet usage had been monitored by her employer (a Welsh College administered by the state). The reason of the monitoring had been to ascertain whether the applicant had been making excessive use of her employer's facilities for personal purposes. The government had in this line admitted that "monitoring took the form of analysing the websites visited, the times and dates of the visits to the websites and their duration"[113] and that "monitoring of emails took the form of analysis of email addresses and dates and times at which emails were sent"[114]. The ECtHR thus held that "[a]ccording to the Court's case law, telephone calls from business premises are prima facie covered by the notions of "private life" and "correspondence" for the purposes of Art.8(1). It follows logically that the sending of emails from work should be similarly protected under Art.8, as should information derived from the monitoring of personal internet usage."[115] And because traffic data are considered to be an "integral element of the communications" the mere

[112] [2007] 45 E.H.R.R. 37 (Copland).
[113] Copland at [11].
[114] Copland at [13].
[115] Copland at [41].

collection and storing of such data does amount to an interference with the right to private life.[116]

In addition, it is important to recall for our purpose that the collection and storage of publicly available information can amount to a prima facie interference with the right to private life in particular when they are done systematically[117].

DPI practices followed by ISPs, whatever their degree of intrusiveness, rely upon the collection of personal data since IP addresses, within the hands of ISPs, at least can be considered as personal data within the meaning of the data protection Directive and Article 8 of the European Charter[118]. Moreover when DPI practices rely upon the collection of data above the network layer it can be argued that these data "make it possible …. to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period"[119], even if these practices do not necessarily reach application data. It is true that the categories of personal data and information pertaining to the private life of an individual are not necessarily equivalent but by looking at the case law of the ECHR and the CJEU it does seem that at least when the collection followed by the retention of personal data becomes systematic and/or permanent a prima facie violation of the right to privacy is characterised. Besides, in its recent decision the CJEU clearly stated that "[t]o establish the existence of an interference with the fundamental right to privacy it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way"[120].

As a result, it could be argued that whatever the nature of the application used to communicate over the Internet, DPI practices amount to a prima facie interference with the right to private life when they are followed by the retention of personal data. Besides, it is the retention of traffic data which is a concern for the CJEU in the Digital Rights Ireland case. The same should probably be true when DPI practices are followed by automated individual decisions producing legal effects upon Internet users, e.g. restriction upon the exercise of fundamental rights and freedom such as freedom of expression, even though no case can be cited here. Obviously the interference would become more serious if application data were to be collected and stored.

Truly a prima facie interference to the right of private life can ultimately be found lawful if it passes Article 8(2) scrutiny. In this line, the ECtHR has already ruled that when it comes to secret surveillance practices by law enforcement agencies several legal safeguards must be present within the legal framework at stake: "[i]n its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed"[121].

Strictly speaking, DPI practices if not triggered by law enforcement agencies are not tantamount to secret surveillance practises. It could however be argued that Convention members have a

---

[116] Copland at [43]-[44]. Ultimately in this case because no laws clearly detailed the way in which employers could monitor the communications of their employees the interference could not be justified under Article 8(2).

[117] See e.g. Leander v Sweden (1987) 9 E.H.R.R. 433 at [19]; Segerstedt Wiberg v Sweden (2007) 44 E.H.R.R. 2 at [72]; Rotaru v Romania (2000) 8 B.H.R.C. 449; Von Hannover v Germany [2004] E.M.L.R. 21 at [95]. See also Copland at [43].

[118] Sabam at [51].

[119] Digital Rights Ireland at [26]. In this case the interference with the right to private life was held to be particularly serious. Digital Rights Ireland at [37].

[120] Digital Rights Ireland at [33].

[121] Kennedy v United Kingdom (2011) 52 E.H.R.R. 4 at [95].

positive obligation[122] to make sure that when communications service providers engage in systematic monitoring practices for legitimate purposes (such as managing traffic, ensuring network security, enforcing copyright law) legal safeguards should nonetheless be present within the legal framework to ensure DPI practices do not amount to the de facto building of user profiles or are not followed by automated individual decisions without the implementation of suitable measures to safeguard Internet users' legitimate interests.

At this stage different routes could be followed if one wants to go beyond the listing of the principles of finality, data minimisation and limited duration. As illustrated by table 1, the first way to confine DPI practices would be to prohibit the retention of traffic data on top of the collection of the content of communications[123]. Such a prohibition could however in some cases undermine the usefulness of legitimate DPI practices in relation to traffic management and network security. A point to note here is that in order for ISPs and other organisations to be able to collaborate and work together to minimise the spread and impact of malware, it is necessary to both perform DPI (to detect the systems infected with malware, or the systems acting as command and control servers) and to then share information (including IP addresses) about those systems. In particular it is useful for these purposes to create black lists of "bad" IP addresses (hosting malware command-and-control servers) and have DPI applied for these IP addresses to see if the content being accessed is really bad (as Cleanfeed does). There is thus some 'tussle' between a user's privacy, and the desire to minimise malware on the network.

The second possibility would then be to limit the scope of the prohibition to collect and retain data to the content of communications with eventually an exception for IDS and require the anonymisation of traffic data or certain types of traffic data. It would then be necessary to determine how effective the anonymisation technique should be, which is not an easy task. Indeed, it is arguable that replacing IP addresses by random numbers is insufficient to claim that the traffic data are anonymised. In its recent opinion on anonymisation techniques the Article 29 Data Protection Working Party[124]stated that anonymisation techniques should aim at irreversibly prevent identification. It takes into account three criteria to assess the robustness of such techniques: the singling out of an individual, linkability, and inference: "[a]n effective anonymisation solution prevents all parties from singling out an individual in a dataset, from linking two records within a dataset (or between two separate datasets) and from inferring any information in such dataset"[125]. As a result it is not enough to simply remove a directly identifying element[126]. In addition it is arguable that the anonymisation of traffic and content data would diminish the usefulness of these data.

The third option would be to require service providers to physically bind the traffic data retained with the legitimate purpose pursued and strictly limit the conditions for transfer and access to these data by for example requiring a prior judicial decision or that of an independent administrative authority[127] while setting oversight mechanisms and imposing security obligations. This option would be the sole way to preserve data retention obligations. More importantly, this

---

[122] Positive obligations have been recognised in several cases. See e.g. Van Kück v Germany (2007) 37 E.H.R.R. 51 at [71]. See also Mosley v United Kingdom (2011) 53 E.H.R.R. 30 at [120], Karakó v Hungary (2011) 52 E.H.R.R. 36 at [19], Von Hannover (2005) 40 E.H.R.R. 1 at [57]; Rees v United Kingdom (1987) 9 E.H.R.R. 56 at [37]; Gaskin v United Kingdom (1989) 12 E.H.R.R. 36 at [42].

[123] This notion could cover both traditional correspondences and browsed information.

[124] Anonymisation Techniques, p. 7.

[125] Anonymisation Techniques, p.9.

[126] In addition, if the data controller does not erase the identifiable personal data, the anonymised data is still personal data.

[127] The CJEU in the Digital Rights Ireland case notes that "the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits". Digital Rights Ireland at [63].

would allow the sharing of "bad" IP addresses among organisations like Team Cymru[128]. Here the problem would be to identify and implement robust binding techniques. It is also worth recalling that the CJEU seems quite demanding in terms of security measures. In the Digital Rights Ireland case it seems to imply that the storing of personal data within the European Union is an essential safeguard and that the taking into account of economic considerations to determine the level of protection of personal data does not ensure that a high level of protection will be ultimately reached[129].
A second type of safeguard could be needed in cases in which DPI practices are followed by automated individual decisions in order to inform users of the reasons for the decisions and give them an opportunity to oppose them.

Content data / **Traffic data**	Prohibition of collection and retention	Prohibition of collection and retention with an exception to run IDS (allowing both collection and retention)
1. Prohibition of retention of traffic data	Solution 1a	Solution 1b
2. Anonymisation of traffic data	Solution 2a	Solution 2b
3. Introduction of a mechanism to physically bind the traffic data retained with the legitimate purpose pursued as well as the laying down of strict limitations for the transfer and access to these personal data (e.g. only to law enforcement agencies if warrant), oversight and security obligations.	Solution 3a	Solution 3b

Table 1: Legal safeguards for the confinement of DPI practices in relation to the nature of the data at stake.

By way of example it is interesting to note that Article L34-1 of the French Postal and Electronic Communications Code (PECC) provides that as regards traffic data as such, the duration of the retention period for the purpose of safeguarding the security of the network cannot exceed 3 months. In addition, information allowing the identification of subscribers cannot be retained for this purpose[130]. With this said, it is also mentioned that ISPs shall not in any case use and retain the content of exchanged correspondences or the content of consulted information, even if the purpose pursued is that of the security of their networks and even if consent has been obtained on the part of their subscribers[131]. While it would seem at first glance legitimate to prevent ISPs from using the content of communications and consulted information for security purposes, in some cases, as aforementioned, ISPs would find it useful to inspect the payload of incoming (from server to client) and outgoing (from client to server) packets.

[128] http://www.team-cymru.org/, accessed June 28, 2014.
[129] Digital Rights Ireland at [67]-[68].
[130] Art. R10-14 of the PECC.
[131] "Elles [les données conservées et traitées] ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications". In France though data retention obligations extend to over-the-top service providers and in particular hosting providers.

With these safeguards in mind, it is now possible to assess the legitimacy of current or past DPI practices. To the extent the Cleanfeed system does not combine the URLs visited with the IP address of the users to then retain the data then it is a more legitimate technology than Detica CView although they both rely upon the inspection of application data. With this said, remains the question of the information of Internet users who in principle should be made aware of the restrictions affecting their Internet accesses and ultimately that of the real effectiveness of the technology in practice[132].

Conclusions

It has been suggested by some commentators that DPI Internet surveillance should be placed in the context of the post-9/11 moral panic about terrorism, and thus be conceived as a part of the "political-economic complex that combines profit interests, a culture of fear and security concerns".[133] The Snowden revelations have also raised public awareness of the monitoring activities and capabilities of governments. With this said, it is certainly striking to note that the legitimisation of DPI practices does not only come from the top, governments engaged in data surveillance, but also from the bottom by judges mainly concerned about content regulation and in particular enforcement of copyright law. The latter are indeed far from cyber-security dilemmas and yet monitoring the behaviour of every user to prevent copyright infringement does not seem to be much of a problem.

The implementation of DPI technologies to reduce copyright piracy however marks however a shift of paradigm: every user gets monitored to make sure that service providers can detect and react to infringements.

The only clear outer-limit set by the CJEU in this field is that it is not possible to actively monitor the content of all the communications on one's network. It is arguable whether such a limit will ever be relevant since by looking at the way the technology functions, in several scenarios only one part of the communications is actively monitored. On occasion national judges have even argued that technically speaking it is not possible to speak about active monitoring since content data is never really inspected.

Besides, the e-privacy Directive does not seem to clearly frame the processing of personal data for traffic management and network security purposes. What is more, while the concept of content of communications is to some extent ambiguous, that of traffic data is very broad and does not exactly correspond to metadata in as much as it includes elements of the packet payload.

It is therefore crucial to make sure that appropriate safeguards are put in place to avoid the creeping extension of surveillance practices.

If far-reaching data retention obligations remain into place little can be done to really confine the development of these practices. Even if such obligations are to be limited in scope it is difficult to come up with effective safeguards. This is all the more true that DPI practices are in some cases legitimate as long as there is no retention of tracking information or no possibility of re-use of the information.[134]

It is suggested nonetheless that the two main criteria to be taken into account to scrutinize DPI practices are the subsequent retention of personal information and the issuance of automated individual decisions having legal effects upon Internet users. This would allow taking seriously the CJEU's holding in the Digital Rights Ireland case, which seems to be implying that both the obligation to retain traffic data and the de facto retention of traffic data is problematic in

[132] See in this regard IFPI, "Digital Music Report 2014", March 2014, accessed March 28, 2014, http://www.ifpi.org/downloads/Digital-Music-Report-2014.pdf.

[133] Fuchs, "Societal Impacts of Deep Packet Inspection Internet Surveillance", 1330.

[134] See e.g. the interesting case of AMP v Persons Unknown [2011] EWHC 3454.

particular when it is done in a systematic manner. The Sabam and Netlog cases should thus be read together with the Digital Rights Ireland case.
More generally, it is debatable whether it is enough to rely upon the good will of service providers to make sure profile building is not the result of the processing of personal data including content data. In this line, it is to be regretted that the CJEU did not follow the opinion of the Advocate General in the UPC Telekabel case and did not require judges issuing injunctions against Internet intermediaries in copyright cases to scrutinize the technology used to implement in practice the judicial order.[135]

[135] UPC Telekabel at [52].