Network neutrality and privacy according to art. 8 ECHR

Koops, E.J.; Sluijs, J.P.J.B.

Published in:
European Journal of Law and Technology

Document version:
Publisher's PDF, also known as Version of record

Publication date:
2012

EJLT European Journal of Law and Technology

Network Neutrality and Privacy According to Art. 8 ECHR

Bert-Jaap Koops [1], Jasper Paul Sluijs [2]

Cite as: Koops, B-J, Sluijs, JP 'Network Neutrality and Privacy According to Art. 8 ECHR', European Journal for Law and Technology, Vol. 3, No. 2, 2012

This article presents a structured approach to studying the privacy implications of the network neutrality debate according to art. 8 of the *European Convention of Human Rights* (ECHR). Network neutrality is a topic discussed in telecommunications policy circles, on how actively Internet Service providers (ISPs) may manage the traffic of content on their networks. While more active network management may lead to more efficient bandwidth allocation, it also strengthens the gate-keeping position of ISPs—with possible negative effects in terms of fairness. It is often alleged in European public interest circles that network management that goes beyond 'neutral' handling of traffic violates the privacy of Internet users. However, such claims are mostly rhetorical in character and are typically not supported by legal research. We attempt to fill this lacuna by comparing network neutrality related privacy claims to art. 8 ECHR case law. Our findings suggest that an art. 8 ECHR violation due to network management is not as straightforward as sometimes assumed, and mainly depends on the form and technique of network management, and the level of State involvement in network management.

1. Introduction

Network neutrality is a contentious topic in telecommunications policy. In short, the debate on network neutrality concerns the amount of 'network management' that Internet Service Providers (ISPs) should be allowed to perform on their networks. With the advent of broadband has come a demand to manage Internet traffic in a differentiated, non-neutral manner, depending on the content of traffic. For instance, in order for YouTube videos to buffer faster, some less time-sensitive traffic may have to be slowed down. More active network management by ISPs may indeed allow for more streamlined Internet usage by consumers, however, it also reinforces the gate-keeping position that ISPs have vis-à-vis content providers and end-users on the Internet, with possible adverse effects for competition and civil rights.

Network neutrality has originated as a discussion in the US, but has also become relevant in a European context. European policymakers have approached network neutrality mainly from an economic perspective, and the European regulatory response to the network neutrality discussion has therefore mainly been aimed at enhancing competition by a light-touch transparency policy. This regulatory approach fits within the broader scheme of European telecommunications regulation, which is heavily premised on economic principles. Ever since the progressive liberalization and privatization of the telecommunications sector, European telecommunications policy has been progressing towards the (ideal) situation in which telecoms are only subject to competition law, without any sector-specific regulation being necessary.

However, European civil-society pressure groups have made attempts to reject the economic approach to network neutrality regulation, and focus on the effects that non-neutral network management by ISPs has on fundamental rights such as freedom of expression and privacy. [3] With ISPs in a stronger gate-keeping position, the freedom of citizens to receive and impart information and the secrecy with which they can communicate are negatively affected, according to this rationale. This fundamental rights approach to network neutrality has made inroads in European policy circles, particularly the European Parliament, and has even been included in revised European telecommunications regulation. [4] [5] In contrast to the US, however, there has nevertheless been little, if any, significant legal research into how valid the claims that non-neutral network management undermines European fundamental rights really are.

With this article, we have made an attempt to offer a structured approach to assessing the merits of European fundamental rights claims in relation to network neutrality. The present research asks if and to what extent network management that departs from 'neutral' principles violates European privacy rights according to art. 8 of the *European Convention of Human Rights* (ECHR), which guarantees the respect for family and private life. We suggest answers to this question by providing an extensive analysis of art. 8 ECHR case law, which we relate to different kinds of network management. The Convention is the major European legal document on Human Rights, and the Court enforcing these rights has developed a sizable case-law on privacy matters. This makes ECHR jurisprudence the logical starting point to discuss the merits of European fundamental rights claims concerning network neutrality. It should be stressed, however, that art. 8 ECHR is by no means the only or most important source of European privacy law. This article will therefore not draw conclusions regarding 'the' European privacy implications of the network neutrality debate, but merely focus on the impact of privacy according to the Convention on network neutrality.

In terms of methodology, we distinguish between what the literature on network neutrality has defined as the three most common types of network management—blocking, degrading and prioritising of traffic—and furthermore whether or not such network management is premised on Deep Packet Inspection (DPI) technology. Then, where possible, we test these forms of network management against the two paragraphs of art. 8 ECHR: assessing first whether different forms of network management constitute an interference with privacy according to art. 8(1), and second whether this interference, once established, is in accordance with the law; carries a legitimate aim; and is necessary in a democratic society according to art. 8(2).

The remainder of this Article will be structured in the following way. We will start off with a short literature review on the topic of network neutrality, identify various forms of network management, and relate the network neutrality debate to the European regulatory response thereto. This will lead into a description of what prompted the present research: the attempts of European public interest groups to frame network neutrality in terms of fundamental rights rather than the law and economics framework through which policymakers have approached the issue. We will then proceed to focus on one European fundamental right in particular, the right to privacy as enshrined in art. 8 ECHR. What follows is an extensive analysis of whether, and to what extent, art. 8 is of relevance for the network neutrality debate. We shall analyze if and how three common forms of network management—blocking, degrading and prioritising of traffic—could constitute a violation of privacy by following the legal test that the European Court of Human Rights (ECtHR) has developed in art. 8 proceedings.

Our findings suggest that only in a minority of cases it is likely that extended network management by ISPs will lead to a violation of art. 8 ECHR. A violation is mainly dependent on whether or not Deep Packet Inspection is utilized by ISPs as a network management technique, and whether or not traffic is blocked. Another key relevant factor is the role public authorities have in (mainly) blocking of network traffic—increased public involvement, for instance mandated filtering of copyright infringing or indecent material, will make a violation more probable. However, we acknowledge that our conclusions are speculative, and based on analogies with alleged privacy violations relating to older media of the art. 8 case law—such as telephony or written correspondence. Our findings are therefore not intended to be definitive, but rather meant as part of a broader research agenda on network neutrality and European privacy law. As stated above, the study of network neutrality from the perspective of European fundamental rights is an underdeveloped field in legal academia. Our aim with this article has been to initiate a constructive methodology to researching the impact of art. 8 ECHR on network neutrality, and we invite others to build upon this endeavour by applying our methodology to other sources of European privacy law.

2. On Network Neutrality

Over the last decade the network neutrality debate has shaken up the traditionally technical and specialist field of telecommunications policy into a more polarized policy area than ever before. In short, the network neutrality debate concerns the trade-off between allowing Internet Service Providers (ISPs) to differentiate their traffic and manage their networks more actively, and the possible exploitation by ISPs of their gate-keeping position. [6]After all, ISPs function as the platform between end-users and content and service providers such as Google and Facebook, and could exploit this position for anticompetitive purposes. [7] At the same time, with the advent of broadband Internet services has come a legitimate demand for not all traffic to be treated equally. Some traffic—say, HD live video streaming—is more sensitive to jitter and delay than other traffic, such as e-mail. This in contrast to the original architecture of narrowband Internet, where

all traffic was of approximately the same 'weight' and could therefore be treated in a more egalitarian manner. [8]

Network neutrality thus touches upon the common debate between fairness and efficiency, [9] and as such has become a polarized debate between proponents and opponents. [10] Unsurprisingly, there is little academic consensus on the topic, which has prompted academics to publish a surge of literature on network neutrality, both in the fields of law, economics [11] and engineering. [12] [13] [14] A key point in the network neutrality debate is how much 'network management' ISPs should be allowed to perform, and whether a balance of appropriate network management should be obtained through market forces or by regulation. The literature highlights three specific forms of network management that are considered problematic: blocking, degrading and prioritising of Internet traffic. [15]

Blocking of traffic is rather self-explanatory: an ISP would completely prevent certain traffic from reaching end-users by for instance dropping packets or inserting reset packets within traffic. In some cases this is desirable, for example in battling spam or malware, while in other cases blocking can be regarded as undesirable—for instance when telecom operators block skype on mobile broadband. [16] Degrading of traffic can be interpreted as partial blocking: the ISP deliberately slows down packets of certain content and service providers so that end-users have trouble receiving this content as originally intended. ISPs could for instance slow down BitTorrent or other P2P traffic because this protocol consumes too much bandwidth. In case of filesharing of copyright infringing material this may be warranted, however, the P2P protocol is also widely used for legal purposes. Finally, ISPs can resort to prioritising certain traffic over others. As alluded to above not all traffic is equally prone to delay, which would only make it logical to prioritise time-sensitive applications such as streaming video or telemedicine services over less time-sensitive applications such as e-mail. [17] However, especially in situations of vertical integration—say, an ISP that is also active as a content provider—ISPs may be incentivized to prioritise their own vertically integrated subsidiaries over competing downstream services, which qualifies as foreclosure. [18]

The debate on the legitimacy of blocking, degrading and prioritising of traffic initially took place in US policy circles, but has gradually extended to Europe and other parts of the world. [19] [20] In fact, the network neutrality debate reached Europe right at the time when the EU institutions were in the process of revising European telecommunications law, which is a highly harmonized field of EU law. [21] Ever since the progressive liberalization and privatization of the sector, telecommunications regulation has become heavily premised on an economic approach to policymaking. This has led to a system in which telecommunications preferably are subject to ex-post antitrust oversight only, with the ambition to completely phase out all ex-ante regulation in competitive markets. [22] Only in case of so-called Significant Market Power (SMP) of a telecommunications provider is the aforementioned broad suite of telecommunications directives available to mitigate this SMP, however, such regulation should be rolled back as soon as the market in question becomes competitive again. [23]

This mechanism of 'ex-post triggered ex-ante regulation' was devised to intervene as little as possible in dynamic telecommunications markets, and as such also seems an appropriate approach to emerging markets such as broadband. [24] The European institutions have therefore considered regulation on the topic of network neutrality with due prudence, and have eventually settled for a light-touch approach of transparency regulation. [25][26] While it goes beyond the scope of this paper to evaluate whether or not this transparency policy is appropriate in dealing with network neutrality concerns, in any case transparency fits within the overall economic approach to telecommunications regulation that the EU has fostered. [27] However, while policymakers have advanced an economic approach to network neutrality, the European public interest community has consistently approached the topic in terms of fundamental rights. Activist groups throughout Europe have mainly interpreted increased network management by ISPs as potential threats to fundamental rights such as freedom of expression and privacy. [28] [29] In the following section we will go deeper into these assumptions and relate this to European fundamental rights law.

2.1 Network Neutrality and European Fundamental Rights

Interestingly—and notwithstanding the traditional economic approach to telecommunications regulation—particularly the European Parliament has been receptive to this fundamental rights approach to network neutrality brought forward by the public interest community. [30] Given the European Parliament's traditional interest in human rights matters related to online technology—particularly privacy [31] — this is not surprising. This focus of the Parliament on fundamental rights eventually resulted in an unusually explicit

reference to the *European Convention of Human Rights* in the *Framework Directive*. [32] At the same time, the National Regulatory Authorities (NRAs) who are essential in enforcing European telecommunications regulation have in turn indicated they lack the competence to adjudicate network neutrality disputes related to fundamental rights. [33] This prompts questions as to what status referrals to fundamental rights within the Framework really have, and how provisions like the following will work in practice:

> Member States wishing to implement measures regarding end-users' access to and/or use of services and applications must respect the fundamental rights of citizens, including in relation to privacy and due process. [34]

Therefore, even though bold statements on how some forms of network management affect fundamental rights are quite common in public interest circles, [35] it is not altogether clear how network neutrality and European fundamental rights law relate to each other. American constitutional law scholars have developed a sizable literature on network neutrality in relation to US fundamental rights. [36] However, such a literature is lacking altogether in European legal academia. [37]

It must be acknowledged nevertheless that in an Internet context fundamental rights carry a strong rhetorical meaning. The Internet is widely regarded as a medium affording interaction and communication on an unprecedented scale, with far-reaching implications for traditional interpretations of basic human rights and public values such as privacy, freedom of speech, secrecy of communication and data protection. [38] There thus seems to be a demand for more thorough legal research into the merits of fundamental rights claims in a network neutrality context. At the same time European telecommunications policy, which includes Internet policy, has arguably been subject to economic determinism in which the supposed relevance of fundamental rights has received little attention—both by policymakers and by academics. The present article explores only one angle of the unexplored field of European fundamental rights and network neutrality: privacy according to art. 8 ECHR. The relevance of this angle shall be motivated in the following section.

2.2 Legal Framework of Fundamental Rights in Europe

The alleged economic determinism of European telecommunications policy calls for more systematic research into the relevance of European fundamental rights law for the European network neutrality debate, beyond the rhetoric of the public interest movement and the European Parliament. The first and obvious step would be to identify exactly which European fundamental rights are at stake in the network neutrality debate, and according to what legal framework. To start with the latter, both the phrasing of the new *Framework Directive* [39] and the of the public interest community [40] as it turns out seem to rely on the wording of the European Convention on Human Rights (ECHR) by using terns like 'necessary in a democratic society' and 'public interference.' The Convention and the case law that comes with it thus seem like a logical starting point to assess the merits of European fundamental rights claims in relation to network neutrality. Indeed, the ECHR is the central document for European Fundamental Rights, [41] and the *EU Fundamental Rights Charter* is based on it. [42]Moreover, with the adoption of *Lisbon Treaty* it was decided that the EU will accede into the ECHR, and in general the EU treaties testify of a high regard for European fundamental rights such as the Convention. [43] [44]

The natural next question would be which ECHR articles have a potential effect on the network neutrality debate. Considering the public interest position papers freedom of expression (art. 10 ECHR) and the right to privacy (art. 8 ECHR) come to mind rather intuitively. [45] [46] This would imply that increased or decreased network management by ISPs somehow has an effect on how citizens are able to receive or impart information, and the privacy with which they can communicate. A less intuitive ECHR right at stake with the network neutrality would be the freedom of assembly and association. Here, ISP network management would have an effect on the ways in which citizens are able to organize themselves and protest on the Internet, [47] which according to anecdotal evidence is by no means a hypothetical concern. [48] We find that at this point particularly privacy and freedom of expression warrant further research, as these fundamental rights seem to lead to most concern in the European network neutrality debate. In the present paper we wish to focus on privacy according to the Convention, while freedom of expression will be addressed by one of the authors in a separate paper. [49]

Before we start our art. 8 ECHR analysis, it should be stressed at the outset that fundamental rights offers a specific angle to disputes that concern network neutrality, alongside European or national telecommunications regulation and general competition law. All these legal regimes are in principle relevant

for the network neutrality debate, and no perspective prevents stakeholders from invoking any of the others in a policy-making process or a legal procedure. As such, by no means do we argue in this article that network neutrality is or should be a matter of fundamental rights exclusively. By the same token, there are many more European sources of privacy law beyond the ECHR, such as the *Data Protection Directive*; the *Electronic Privacy Directive*; the *Data Retention Directive*; [50] [51] [52] and the Charter of Fundamental Rights of the EU, to mention only a few. [53] As this research focuses on the ECHR, its conclusions will also only concern the validity of privacy claims according to the ECHR related to network neutrality. The scope of this research project does not allow us to draw conclusions on the effects that European privacy law in general have on network neutrality, and this article is therefore also not intended as such.

3. Analysis

3.1 Privacy

Art. 8 ECHR guarantees the right to respect for privacy, formulated as follows:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The structure of art. 8 is the same as that of arts. 9-11 ECHR: paragraph one provides a general description of the right, whilst paragraph two lists conditions under which an interference with the right is allowed. Since the notion of private life is a broad concept that includes relationships with the outside world, and since correspondence also covers Internet communications, it is clear that privacy is potentially an issue when Internet Service Providers actively manage Internet traffic. [54] [55]

Given the aforementioned claims of public-interest organizations, our analysis will mainly focus on alleged art. 8 violations of natural persons. However, given that art. 8 has 'by far the widest scope' of the Convention, to some extent art. 8 ECHR also covers legal persons. [56] According to art. 8 ECHR jurisprudence a privacy violation *stricto sensu* can only be brought by a natural person, not by legal persons—this in contrast to, for instance, art. 10 on freedom of expression. At the same time, legal persons do enjoy protection under the Convention regarding the privacy of their home and correspondence, although 'such protections may be strictly confined to company premises.' [57] [58] [59] This seems to suggest that art. 8 ECHR may be difficult to apply to content and service providers such as Facebook and Google. [60] We shall therefore assume for the remainder of this article that complaints have been brought by individuals. To determine whether and to what extent network management violates the Convention's right to privacy, the steps of art. 8 ECHR have to be analysed. First, is there an interference with the right to privacy (paragraph 1), and second, if this is the case, is the interference legitimated by fulfilling the criteria of paragraph 2 of art. 8? For this we will draw analogies between network management practices and existing art. 8 case law, to compare this jurisprudence to (hypothetical) network neutrality matters.

3.1.1. Paragraph 1: Interference

According to art. 8(1), the exercise of the right to privacy shall not be *interfered with by a public authority*—unless the criteria of art. 8(2) are met. For an infringement of the right to privacy under the ECHR, two questions therefore have to be answered: when does network management constitute an interference with people's exercise of their right to privacy, and is this interference done by a public authority?

When does network management constitute an interference?

Despite the claims made by some public interest groups that deviations from network neutrality are a threat to privacy, [61] it is far from evident that privacy according to the ECHR is an issue in network management. Most concerns are raised by Deep Packet Inspection (DPI), which is said to be a useful, perhaps necessary, tool to perform network management.

DPI-based network management

DPI is a powerful network engineering technique with a potentially endless number of applications. Traditional, 'shallow' packet inspection systems can identify and monitor traffic only based on the headers of Internet traffic, which is analogous to the envelope of a letter. DPI however can go all the way down to the deepest (application) level of Internet packets according to the OSI model, so that program, software or protocols being used can be identified in real time, and crucially, to determine what these applications are being used for. [62] [63] This implies that DPI technology allows for the screening of content by third parties, including web browsing, email, and VoIP calls. [64]

DPI enables ISPs to ensure network security, perform network management, and to achieve price discrimination, behavioural advertising or content filtering. [65] [66] [67] In general, DPI seems a more refined tool for network management, regardless of the specific purpose, as it enables ISPs to better distinguish between packets. It should be borne in mind, however, that, although helpful, DPI does not seem necessary for many typical network management purposes. [68] The many ways in which DPI can be applied for network management and other functions does however not lead away from the fact that in many instances the actual content of communication is being monitored by a third party, the ISP. [69] The possibility to communicate without being intercepted is a fundamental element of privacy, specifically mentioned in art. 8(1) as respect for correspondence.[70] If DPI is used and thus correspondence is intercepted by the ISP, there is a clear interference with users' right to privacy.

Non-DPI-based degrading or prioritising traffic

The situation is less clear, however, when network management does not involve DPI. Let us suppose network management is based on shallow packet inspection. We will analyze first network management in the form of degradation or prioritisation, and subsequently network management in the form of blocking. When asking whether degrading or prioritising traffic touches upon the right to privacy, we can look at three possible arguments. The first is that managing traffic involves processing of personal data. If prioritising or degrading traffic is based on sender or receiver, then IP addresses will be processed, which, according to the Article 29 Working Party, are to be considered personal data. [71] [72] Personal data are included in the scope of art. 8(1) ECHR, and data protection is increasingly being considered part and parcel of the right to privacy by the ECtHR. [73] If network management is based on type of traffic, however, such as streaming audio or video or instant messaging, this as such does not involve processing address information or content, and hence does not involve processing of personal data.

The second argument is that managing traffic involves processing of traffic data, i.e., any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. The processing of traffic data may touch upon the right to respect for correspondence and hence falls within the scope of art. 8(1) ECHR. [74] Some types of data processing are not an interference, for example, the provider's processing of traffic data for billing purposes. [75] In *Malone*, the Court found an infringement of art. 8(1) because the traffic data were provided by the telecom operator to the police. [76] In *Copland*, the Court noted that processing traffic data can also constitute an interference when they are not disclosed or used against the person in disciplinary proceedings. [77] What is relevant is how the traffic data are used, which in this case—with storage of traffic data over an extensive period of time by the employer who suspected Copland of excessive use of communication facilities—constituted an interference. [78] From this case-law, we can infer a criterion for interference being that traffic data are processed in another way or for other purposes than for their primary purposes of routing traffic and billing.

Is it possible to distinguish systematically between network management of traffic data primarily for billing and routing, and other forms of network management? The issue is whether network management involves processing of packets for a primary purpose (the conveyance of a communication or billing) or rather for a derivative purpose (the manner of conveyance of a communication). Existing research distinguishes between traffic data and communication content, where traffic data concerns the three essential functional tasks of ISPs, and three types of services that ISPs perform. [79] The functional tasks of ISPs are:

- service performance—processing of data as part of the service agreement with a consumer;
- service management—processing of data for the purpose of traffic management and maintenance of the network; and
- service accounting—processing of data for billing purposes,

while the service types are: [80]

- mere conduit—facilitating transmission on, or access to a communications network;

- caching—automatic, temporary and transient storage of data to streamline transmission; and
- hosting—facilitating the storage of data by consumers on the ISPs premises.

The crucial difference between traffic data and communications content is that when at least one of the functional tasks is performed by an ISP for the purpose of at least one of the service types, the ISP is involved in handling traffic data. When this is not the case, the ISP will handle communications content instead. [81]

This typology provides a useful heuristic for assessing whether traffic management involves data processed for a primary purpose (i.e., processing traffic data that are essential for the service) or for a derivative purpose (processing communications content), which allows us to apply the *Copland* rationale to ISPs' network management practices. Network management for the purpose of degrading or prioritising of traffic is done for the service type of mere conduit, and performs the function of service management ('data processing for traffic management and network maintenance') and perhaps also the function of service performance ('data processing to perform the service agreement with the user'), if the contract contains for example performance levels. Hence, such network management involves processing of traffic data for their primary purpose. [82] This would imply that network management uses traffic data in a way that may not infringe art. 8(1) according to the *Copland* standard.

An alternative argument would be that traffic degradation or prioritisation does not infringe privacy because personal or traffic data are processed, but rather because of some more general privacy concern. After all, art. 8 has been interpreted in a dynamic way by the Court taking into account current scientific and social developments, and the notion of private life is a broad concept not susceptible to exhaustive definition. [83] [84]

One approach would be that degrading network traffic hampers the delivery of correspondence. There is a significant body of art. 8 case law on correspondence of prisoners; although initially the ECtHR did not consider delay of correspondence an interference under art. 8(1), later on the Court came to the conclusion that more types of restriction on correspondence of prisoners fell within the scope of art. 8(1). [85] [86] Nevertheless, we do not think that the case-specific circumstances of these restrictions—preventing a prisoner from writing a petition; supervising correspondence of prisoners [87] —can be fully compared to degrading network traffic with shallow packet inspection, which seems much less of an interference with correspondence—unless email, chat or IM are degraded specifically. Altogether, however broad and flexible the notion of private life may be in art. 8(1), we conclude that slowing down or speeding up communication packets does not generally touch upon people's right to privacy. It seems that only when degrading or prioritising traffic is based on sender or recipient information—IP addresses—or when the management goes beyond what is reasonable for routing and billing traffic, that art. 8(1) can be invoked.

Non-DPI-based blocking

Deviations from network neutrality in the form of blocking traffic are much more likely than degradation or prioritisation to infringe upon the right to privacy. The three arguments discussed in the previous section carry more weight here, since blocking is a much more significant interference with correspondence than delay or supervision. [88] Blocking traffic is also less likely to fall under normal service management or service performance, so that the data on which the blocking is based are not processed as normal traffic data; the secondary use of traffic data for the purpose of blocking is more likely to be considered an interference with correspondence. [89] Finally, blocking will often be performed on the basis of content (e.g., unlawful material) or on the basis of sender or recipient information (e.g., copyright-violating file-sharing), both of which can count on the protection of art. 8(1). It should be stressed at this point that there may indeed be cases—think of spam or other malware—in which blocking behaviour may be considered as not violating privacy according to art. 8 ECHR, based on the proportionality test of art. 8(2). This will be discussed below.

Is the interference executed by a public authority?

The second element necessary for invoking art. 8(1) protection is that an interference is done by a public authority. Like the interference as such, this is not evidently the case in many types of network management, since ISPs are usually not a public authority—with the exception of some European countries where ISPs are (partially) State-owned, such as Sweden and Finland. [90] Art. 10 ECHR jurisprudence suggests that the bar for public interference with Convention rights is relatively low however, [91] and in art. 8 jurisprudence particularly the Court has Stated that public interference and positive obligations of the State—discussed below—blend into each other. [92]

If there is no ownership link between an ISP and the State, the interference can still be performed by a public authority in some cases. If a State puts an explicit legal obligation on ISPs to conduct network management, there is a clear form of State interference, but such laws are relatively rare. [93] There is no obvious legal obligation as such for degrading or prioritising traffic. [94] However, art.

13a (1) of the *Framework Directive* stipulates that service providers must

> take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services. Having regard to the State of the art, these measures shall ensure a level of security appropriate to the risk presented. [95]

Since (information) security comprises both confidentiality, integrity, and availability, ISPs apparently have to take measures to ensure an adequate level of service availability. [96] One could argue that this comprises monitoring bandwidth availability and intervening when traffic throughput is threatened, in which case they could degrade high-bandwidth traffic (such as spam or excessive peer-to-peer file-sharing traffic) or prioritise time-critical traffic (such as voice-over-IP). However, the provision does not constitute a direct obligation to prioritise or degrade traffic, and it provides a legal obligation only for some types of network management in this respect.

For blocking, there are some clearer examples of legal obligations. Some (controversial) laws have been enacted to oblige ISPs to block access to child-pornographic websites, [97] while some courts have ordered ISPs to block access to unlawful content, such as copyright-infringing file-sharing sites. [98] Such court injunctions are, however, relatively rare. [99] More frequent are forms of Internet blocking, notably of child-abuse images, through public-private partnerships in which ISPs voluntarily block access to blacklisted websites. [100] In these cases, a blacklist is often provided by the police, and this seems to be a sufficient connection to speak of interference by a public authority. In *M.M. v The Netherlands*, the police suggested a citizen to record a conversation with the suspect and connected a tape recorder to her phone; the Court determined this to constitute State interference:

> 'Acting as they did, with the permission of the public prosecutor, the police 'made a crucial contribution to the execution of the scheme', as well as being responsible for its inception'. [101]

These considerations apply analogously to voluntary child-pornography blocking schemes, in which the police often makes a crucial contribution to the scheme of blocking (such as a blacklist and the text of a 'STOP' page shown to users trying to access a site), and ISPs seldom embark on these schemes out of their own initiative. [102] Thus, in case of ISP blocking there seems a considerable likelihood that this is an interference by a public authority, both in mandatory and in voluntary forms of blocking, except when the ISP takes the initiative and has no dealing with the police in the execution of the blocking.

Not all types of blocking reach the threshold of State involvement, however. An increasingly prevalent type of network management comprises blocking to prevent access to services that the user has not paid for, e.g., blocking Skype or streaming video for users of a basic mobile Internet subscription. This is the playing field of market forces and freedom of contract where there seems to be no State involvement outside the boundaries of the Regulatory Framework for Electronic Communications. [103] Therefore, these types of network management cannot be considered to be an interference by a public authority. [104]

Positive obligations

Even if there is no interference by the State as such, art. 8 can still be at issue, namely when the State does not take sufficient responsibility for safeguarding that citizens can enjoy the right to privacy. As mentioned above, the Court does not advance a sharp distinction between direct State interference and positive obligations of States to prevent interferences. [105] The positive obligations of the State under art. 8 have been developed in case-law. [106] Most of these cases deal with private and family life, with environmental protection related to the home, or, occasionally, the privacy of correspondence. [107] [108] [109]

In some sense, the respect for private or family life could perhaps be at issue in network management. In *K.U. v Finland*, the Court assumed a positive obligation for the State to ensure an effective system for legal redress for a victim of sexual harassment, which should include the legal possibility to request an injunction to order an ISP to provide address information of the sender of the harassing message. [110] One might argue that, in a similar vein, a victim of child-abuse images must have the legal possibility of going to court to request an order for ISPs to block access to websites containing images of her/him. Thus, there may

be a positive obligation on the State to have a possibility in the legal system for filtering and blocking unlawful content or for notice-and-takedown regimes. However, the analogy might stretch only so far as that *K.U.* requested information about a particular IP address, implying that a child-abuse victim should be able to request blocking of websites containing his own images, which is substantially different from a generic legal duty to block child-abuse images. Note that following this rationale, positive obligations on States under art. 8 ECHR to protect citizens' privacy would lead to the blocking of data.

The reverse situation seems more likely to invoke positive obligations, i.e., when ISPs block content of their own accord. Unless the filtering and blocking is very targeted—and consequently very limited, as filtering systems are usually coarse instruments—false positives ('overblocking') are likely to occur with users being denied access to lawful content or file-sharing websites. [111] If the filtering is based on keywords, or on blacklisted domain names that host both unlawful (child-abuse images) and lawful (adult pornography) material, following ECHR jurisprudence the blocking might touch upon the intimate or family life of web users, since they are being restricted in the right to develop their sexuality. After all, ECHR case law suggests that the blocking must be of such an extent that users' private (lawful) sexual life be systematically and directly affected. [112] One could thus argue that, while State-mandated or State-triggered blocking is likely to constitute State interference, also voluntary but systematic and sweeping ISP-initiated blocking might trigger art. 8(1) through the positive obligations on the State to prevent ISPs from systematically curbing the sexual, private, or family life of web users, if the blocking system is so crude that it continuously and directly affects users' exercise of sexual freedom on the net.

Key to the ECtHR's approach to positive obligations in art. 8 procedures seems to be the 'direct and immediate' link that the Court requires between the measures sought by an applicant and her private or family life. [113][114] In any event the Court has refrained from advancing a broad interpretation of positive obligations in art. 8 matters and States enjoy a relatively wide margin of appreciation. [115] This inevitably leads to a case-by-case approach to positive obligations, depending on specific facts and circumstances. In case of blocking of content by ISPs this link between remedy and privacy must also be established therefore, which does not allow for strong predictions as to how the Court would approach positive obligations in the case of Internet filtering.

Summary

Deviations from neutral network management do not always constitute an interference of the right to privacy by a public authority. On the contrary, the most common types of network management in the form of prioritising or degrading traffic will seldom be an art. 8 issue. Only when the degrading or prioritising is based on sender or recipient information—IP addresses—or when the management goes beyond what is reasonable for routing and billing traffic, is art. 8(1) interfered with. But unless the ISP is (partly) State-owned, the interference is not done by a public authority, and moreover the slowing down or speeding up of packets does not seem a sufficiently severe infringement of the right to privacy that positive obligations can be assumed.

Network management does become an art. 8 issue when it takes the form of blocking. If the blocking is based on DPI, then correspondence is intercepted by the ISP, which is a clear interference with users' right to privacy. Also non-DPI-based blocking is likely to interfere with the right to privacy, as it will usually deviate from normal service management or service performance, and hence processes traffic data for non-primary purposes, which constitutes an interference. Moreover, with blocking there will also usually be a State responsibility, also if the ISP is non-State-owned, because both in mandatory and in voluntary forms of blocking there is often considerable State involvement. If the blocking is not aided by public authorities and taken on the ISP's own initiative, the ISP's interference with users' privacy can invoke positive obligations if the blocking system is crude and systematically hampers users' use of the Internet to develop their sexual life.

3.1.2 Paragraph 2: Justifications

If network management interferes with the right to privacy, the interference is only allowed if it meets the requirements of art. 8(2) ECHR: it must be a) in accordance with the law, b) pursue a legitimate aim, and c) being necessary in a democratic society. In this section, we will mainly focus on blocking network traffic and not so much on prioritising and degrading traffic. As we concluded in the previous section, prioritising and degrading will probably not constitute State interference, except in the case of a State-owned ISP performing this type of network management based on user address information or in a way that goes beyond what is

reasonable for routing or billing. Moreover, since many instances of degrading and prioritising of traffic are unlikely to be considered interferences with user privacy according to art. 8(1) of the Convention to begin with, an extensive 8(2) analysis becomes less relevant in this context. The main exception to this is when degrading or blocking is premised on DPI, but here there is little difference to DPI-based blocking anyway. Therefore, here we will discuss predominantly whether ISP blocking of traffic passes the test of art. 8(2), both in cases of direct State interference and in cases of positive obligations—the Court does not substantially distinguish between these two types of interference, generally performing a similar test under 8(2). [116] In what follows, we will address the three prongs of the art. 8(2) test.

Is the interference in accordance with the law?

If ISPs block traffic because a law obliges them to do so, then there is a clear enough legal basis. [117] If a court orders an ISP to block certain traffic, this will also normally constitute a clear legal basis. [118] The same goes for prioritising and degrading—assuming this network management constitutes an interference according to 8(1)—even though in practice it seems more unlikely to occur. However, having a basis in law is not enough. The interference must be sufficiently accessible to citizens, and this implies that the legal basis has to comply with qualitative criteria: the scope and manner of exercise of the interference must be explained with sufficient precision,[119] and must be made accessible to the public rather than be laid down in internal guidelines. [120] The Court stresses the importance of clarity in light of technological dynamics:

> 'Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is*essential to have clear, detailed rules* on the subject, especially *as the technology available* for use is continually becoming more *sophisticated*.' [121]

Kruslin and Huvig's stress on the quality of the law is relevant for network management, as this practice is more sophisticated and less understandable to citizens than interception of telephony. A difference may be that communications interception is a more severe infringement than blocking, degrading or prioritising even if it is DPI-based, since the content of communications are not heard or read by law enforcement in criminal investigations, but are automatically scanned for routing or blocking traffic. Nevertheless, DPI infringes the secrecy of correspondence and—following *Kruslin* and *Huvig*—will therefore require a reasonable level of clarity for citizens to be able to know how the secrecy of their communication can be interfered with by ISPs based on certain legal provisions.

In laws or court cases mandating blocking, the level of clarity may not be particularly great. The exact type of network management will be detailed in lower regulations or internal instructions, or will be left to the discretion of the ISP. In the Danish case where Telenor was ordered by a lower court to block users from accessing The Pirate Bay, the Supreme Court stressed the discretionary power for the ISP to determine its network management:

> 'Even if it is left to Telenor to choose between different ways of blocking or obstructing the access to the website, the Supreme Court finds that the prohibition and injunction is formulated in a sufficiently clear and precise way. Telenor has chosen to comply with the prohibition and injunction by blocking access to the website at DNS level [i.e., based on routing information]. The defendant [i.e., IFPI, a music-rights organisation] has Stated that the blocking mentioned is sufficient to comply with the prohibition, and that if the defendant should wish to oblige Telenor to deploy another form of blocking, they can start a new injunction-prohibition procedure, in which a new proportionality assessment is to be made.' [122] [123]

It is questionable, however, whether the Danish court's conclusion in a case about the administrative burden rather than the privacy of blocking—Telenor contested the proportionality of the injunction in terms of compliance costs—can extend to the article 8(2) test of clarity and foreseeability of the law. In *Herczegvalvy*, the Court determined that a law allowing a psychiatric hospital to send letters of its inmates to a curator for selection of which letters would be actively sent out, was accessible but too vague for subjects to foresee the consequences:

> 'These very vaguely worded provisions do not specify the scope or conditions of exercise of the discretionary power which was at the origin of the measures complained of. (…) Admittedly, as the Court has previously Stated, it would scarcely be possible to formulate a law to cover every eventuality (…). For all that, in the absence of any detail at all as to the kind of restrictions permitted

> or their purpose, duration and extent or the arrangements for their review, the above provisions do not offer the minimum degree of protection against arbitrariness required by the rule of law in a democratic society.' [124]

In a similar vein, one can argue that a law or court order mandating for instance ISPs to block certain traffic needs to sufficiently delineate the purpose, duration, and scope of blocking, in order to curb the discretionary power conferred on the ISP. Consequently, if it is left to an ISP whether to conduct blocking at the DNS (based on domain names) or IP level (based on numerical addresses) or by using Deep Packet Inspection, then the scope and manner of the exercise of blocking can hardly be considered sufficiently clear for users. At the least, a court injunction or statutory obligation should make clear whether network management is to be conducted based on routing information—domain names or IP addresses—or on Deep Packet Inspection, as the person concerned 'must moreover be able to foresee its consequences for him.' [125]

With voluntary blocking schemes or other non-public authority ordered prioritising or degrading, it will be harder than with statutory or court-ordered blocking to determine whether the interference is in accordance with the law, as there is no clear legal basis for this. The *Electronic Commerce Directive* for instance can hardly serve as a legal basis. [126] It provides that member States may not impose a general obligation to monitor (art. 15), but allows courts or administrative authorities to require service providers to terminate or prevent unlawful activities (art. 12(3)). This is too far removed from typical public-private partnerships that block unlawful content to be able to serve as a legal basis. Perhaps, in case of voluntary blocking, a basis should be sought in the law criminalizing forms of content. The national criminal provision on child pornography, for instance, would then serve as the legal basis for public-private partnerships that filter child-abuse images. However, having illegal content blocked by one's ISP is considerably removed from the legal provision criminalizing that content. It is questionable whether citizens can foresee the consequences of Internet filtering and blocking on this basis, particularly since a large discretionary power is involved in the decisions what and how to filter. The 'scope or conditions of exercise of the discretionary power' of blocking child-abuse images are not in any way explained in the legal provisions that criminalize child abuse—which is logical, as these are substantive provisions that are not meant to serve as criminal-procedural provisions in the first place. [127]

As a result, we tend to conclude that voluntary network management practices that constitute an interference according to 8(1) ECHR will often not be in accordance with the law, as they lack a sufficiently clear legal basis. Only if some legal provision or lower regulation exists that illegal content must or can be filtered will citizens be able to foresee the consequences of Internet filtering for them. We add a caveat, however, in that there may be a trade-off between the extent of government involvement and the demands made on the quality of the legal basis: the more a public authority is actively involved in blocking illegal content, the more explicit the legal basis will have to be.

And conversely, if the public authority only plays a minor role in voluntary filtering, the legal basis for this may more easily be found in indirect provisions such as criminal sanctioning of child pornography in combination with a general provision in a Police Act that the police has the task of enforcing the law.

An alternative legal basis for blocking, degrading or prioritising of content could be found in legal provisions requiring network operators to safeguard the security or integrity of their networks, such as is formulated in the *EUFramework Directive* concerning electronic communications networks. [128] Such requirements in Directives must be implemented in national legislation. [129] If the basis for blocking, degrading or prioritising content is based on these network integrity provisions, the implementation provision must of course comply with the foreseeability and clarity requirements that the Court has set out, implying that the text should establish a sufficiently clear link between security or integrity threats and the content that is being blocked, degraded or prioritised. For malware and other security threats, such a link will be relatively clear, but for content-related offences, such as child pornography or hate speech, it seems a long shot to argue that such content can be blocked because it threatens network security or integrity.

Does the interference serve a legitimate aim?

Network management can serve different purposes. One frequently occurring purpose—particularly in relation to State interference, such as laws or courts mandating filtering—is to prevent unlawful content from being spread. That is in the interest of the prevention of crime, and hence constitutes a relevant interest for complying with the second prong of the art. 8(2) test. Blocking of harmful but not unlawful material, such as pornographic or violent images that can be harmful to children does not serve the prevention of crime, but it

is presumably done in the interest of the protection of morals or protecting the rights and freedoms of children—or of parents who may want to restrict online content for their young children.

Another purpose of network management, as alluded to above, can be network integrity or security, if the management is focused on either filtering out malware or bulk traffic (e.g., spam or super-high-volume peer-to-peer traffic) that threatens the continuity of service provision. In that case, blocking can be said to serve the interest of the country's economic well-being—the Internet being a critical infrastructure for the economy in the information society—or otherwise for protecting the rights and freedoms of other net users.

Altogether, the second prong of the 8(2) test can fairly easily be accommodated, and in general the Court attaches little weight to this prong anyway. [130] There is, perhaps, one proviso, in that art. 18 States that the 'restrictions permitted under this Convention to the said rights and freedoms shall not be applied for any purpose other than those for which they have been prescribed.' In principle, art. 18 can be violated even if art. 8 itself is not violated. [131] Since 'function creep' is a frequently occurring phenomenon in technological systems and policy, it should be monitored whether network management systems introduced for crime prevention or protecting children are not, gradually over time, used for other purposes in practice, in which case art. 18 might perhaps enter into the equation. [132]

Is the interference proportional?

In most art. 8 assessments, the third prong of art. 8(2) is the million dollar question: is the interference necessary in a democratic society? This is always a case-specific question. As the Court often stresses, the proportionality assessment is made in light of all circumstances of the case, and not meant to provide general assessments on classes of cases. [133] Of course, analogies can be drawn between proportionality assessments of established art. 8 case law and the proportionality of certain types of network management. However, in the absence of cases that specifically address network management, the difficulty of determining whether blocking, degrading or prioritising as forms of network management are necessary in a democratic society is compounded by the fact that most analogies are set in quite different contexts and hence cannot allow us to draw strong conclusions on proportionality. Our conclusions on the necessity of network management are therefore necessarily speculative.

There is a significant case law on the blocking or obstructing of correspondence. However, this jurisprudence is very context-specific: it concerns prisoners, often situations concerning correspondence with a solicitor or with public authorities. [134] [135] The correspondence in these settings is particularly important for the inmates, with few alternative means of communication. [136] This context can hardly be transposed to blocking Internet traffic, where Internet users usually have many communication channels available and where the blocked Internet traffic will often be less vital for the person's well-being than prisoners' correspondence with attorneys. [137]

Having said that, we can offer some remarks about the proportionality of various types of network management, in terms of what is more or less likely to be considered necessary in a democratic society. We can look at several dimensions of the blocking, degrading and prioritising: why, when, how, and by whom this is done—assuming that this form of network management is an interference according to 10(1) ECHR.

First, we have already distinguished between various purposes of network management, blocking in particular: assuring network and service integrity, and blocking illegal or harmful content. The first reason seems relatively non-contentious: ISPs have good reason to filter out Internet traffic containing viruses and malware, and quality-of-service requirements may also imply that bulk spam or high-volume traffic can be blocked. Unless the network management is evidently overdone, we think that this type can often be considered proportional according to 8(2) ECHR. The second reason, blocking unlawful content, may be more contentious, since the dividing line between lawful and unlawful content is much harder to draw than with malware or spam, and automated systems are not particularly precise in only filtering out unlawful content. [138] When it comes to the necessity in a democratic society of network management, we can think of a spectrum ranging from content that is widely and non-controversially regarded as illegal, such as child-abuse images—which will more easily be considered necessary in a democratic society to filter out—to content that is harmful to some user groups but not illegal—which will less easily considered necessary in a democratic society to filter out. [139] [140] Somewhere in between the extremes of this spectrum is copyright-infringing peer-to-peer file-sharing. Although blocking copyright-infringing file uploads is a legitimate aim, this could be considered necessary in a democratic society only if the blocking is very targeted and limited in scope. [141]

This connects to other dimensions, namely when and how the network management takes place. Incidental or short-period forms of blocking or degrading will be more acceptable than generic, continuous blocking systems, as the Scarlet case suggests. [142] Also the granularity of the network management will be a relevant factor. [143] Since filtering systems can never be 100% correct, it will matter whether the system is tuned towards false positives (making sure that most unlawful content is blocked while accepting blocking of lawful content as collateral damage) or towards false negatives (making sure that no lawful content is blocked while accepting that not all unlawful content will be blocked). Obviously, a policy accepting false negatives over false positives is more proportionate for respecting the right to correspondence than the other way around, and as the Court seems to be quite strict when assessing the proportionality of blocking correspondence, this creates a strong presumption that network management systems should tend to false negatives rather than false positives, if they want to be considered necessary in a democratic society. [144]

Finally, it also matters who performs network management, in the sense that the degree of State involvement is likely to influence the proportionality assessment. The more the police, the legislator, or a court for instance is actively involved in blocking illegal content, the stricter the proportionality scrutiny will be. For network management that is done by ISPs with relatively little State involvement (and consequently less privacy interference by a public authority), a larger margin of appreciation is likely to be granted than if the State actively mandates the ISP to block traffic. In short, whether blocking, degrading or prioritising of Internet traffic can be considered proportional in terms of art. 8(2) depends greatly on the circumstances of the case. Relevant factors are the type of content that is 'managed' and the reason for managing this; the duration and scope of network management; the type, granularity, and default settings of network management; and the level of State involvement.

4. Conclusion

Network neutrality is a complex issue that has kept scholars and policymakers busy for around a decade now. Because of the economic premises of European telecommunications regulation, network neutrality has predominantly been approached by European policymakers in economic terms as well. At the same time, the public interest community in Europe rather has actively framed the network neutrality debate in terms of fundamental rights such as freedom of expression and privacy, and particularly the European Parliament had been receptive to this idea. In this article we have discussed the merits of claims that departing from 'neutral' network management affects the privacy of according to art. 8 of the ECHR. The ECHR is a natural focal point for such a research endeavour, as this is the central European legal document on human rights in Europe, and the Court enforcing the Convention has developed a rich jurisprudence on privacy matters.

In contrast to the sometimes bold claims of public interest position papers, we have come to more nuanced findings. First and foremost, we argue against broad, catch-all conclusions of how network management violates the right to privacy according to the Convention. Whether or not ISPs' network management violates the right to privacy as enshrined in the ECHR mainly depends on the form of network management, and the (active) role public authorities play in fostering network management. For instance, unless degradation and prioritisation are premised on DPI technology, it will be unlikely for these types of network management to be considered an interference according to art. 8(1) in the first place. After all, applying *Copland*, it is likely that network management that does not go beyond its primary use—like degrading and prioritising—will not quality for an interference with privacy. [145] Moreover, such network management is very unlikely to be sanctioned by public authorities, and in the absence of a clear interference it also becomes unlikely that the Court would recognize positive obligations here. Blocking of traffic, however, is a different story. Both when premised on DPI and on 'shallow' packet inspection techniques can blocking be considered an interference according to 8(1), as blocking may very well go beyond primary network management purposes. This leads to a situation in which positive obligations on Member States are more probable to be identified by the ECtHR. Furthermore, public authorities are more likely to be involved in blocking traffic by ISPs.

However, we can only draw modest conclusions on whether an interference with privacy according to 8(1) due to network management also becomes a violation of 8(2) ECHR and thus a violation of the Right to Privacy of the Convention. While the 'in accordance with the law' and 'legitimate aim' prongs can fairly easily be dealt with, on the matter of proportionality the case law only allows us to conclude that (not) finding a privacy violation for interfering network management will be a very case-specific affair. The proportionality of privacy-interfering network management depends on matters like the kind of traffic that is managed and the

reasons for this; the duration and scope of network management; its (technical) type and the (programmed) granularity of this technique; and the extent to which public authorities have been involved.

Especially this conclusion on proportionality may not seem spectacular, however, it is useful in the sense that it tones down sweeping claims on the supposed ECHR violations of network management, and offers a road map for more precise study on how different forms of network management have different effects on privacy. Indeed, this research project only covers a small part of the field of European privacy law. We argue for a case-by-case approach to network neutrality in European privacy law, factoring into account the exact and case-specific circumstances of an alleged interference with citizens' privacy. If anything, this article is a call for further and more specific research into assessing network neutrality concerns according to European fundamental rights, and European privacy law.

---

[1] Bert-Jaap Koops is Professor of Regulation & Technology at TILT – Tilburg Institute for Law, Technology, and Society, Tilburg University, the Netherlands.

[2] Jasper Paul Sluijs is PhD Candidate at TILEC – Tilburg Law and Economics Center, Tilburg University, the Netherlands. The authors wish to acknowledge Ronald Leenes and Pierre Larouche for useful comments on previous drafts. The usual disclaimer applies.

[3] ASOCIACIÓN DE INTERNAUTAS, RESPONSE TO THE PUBLIC CONSULTATION ON THE OPEN INTERNET AND NET NEUTRALITY 11 (2010),http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/net_neutrality/comments/index_en.htm. ("The added measure would just be to protect the privacy of users by preventing these practices of the ISPs, governments and corporations and imposing exemplary sanctions to those engaging in the spying of the electronic communications. Right after this habit of spying data, next logical step would be the control of what is allowed and what not (far beyond law) to pass through the Net and the logical consequence of censorship or even worse, selfcensorship by users.")

[4] See amendment 138 to the new Regulatory Framework for Electronic Communications, PARL. EUR. DOC. A6-0321/138 (2008).

[5] *Framework Directive* 2002/21/EC, as amended by Directive 2009/140/EC.

[6] This debate was first brought forward by Mark Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925 (2000).

[7] In economics literature this phenomenon is referred to as a two-sided market, see Jean-Charles Rochet & Jean Tirole, *Platform Competition in Two-Sided Markets*, 1 JOURNAL OF THE EUROPEAN ECONOMIC ASSOCIATION 990-1029 (2003) for a seminal article on two sided markets.

[8] This egalitarian way of routing Internet traffic has become knows as the end-to-end principle, see J. H. Saltzer, D. P. Reed & D. D. Clark, *End-to-end arguments in system design*, 2 ACM TRANSACTIONS ON COMPUTER SYSTEMS (TOCS) 288 (1984).

[9] Andrew Odlyzko, *Network neutrality, search neutrality, and the never-ending conflict between efficiency and fairness in markets*, 8 REVIEW OF NETWORK ECONOMICS 40-60 (2009).

[10] See, e.g. T. Wu & C. S Yoo, *Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate*, 59 FEDERAL COMMUNICATIONS LAW JOURNAL (2007).

[11] B. E Hermalin & M. L Katz, *The economics of product-line restrictions with an application to the network neutrality debate*, 19 INFORMATION ECONOMICS AND POLICY 214-248 (2007); Florian Schuett, *Network Neutrality: A Survey of the Economic Literature*, 9 REVIEW OF NETWORK ECONOMICS (2010). For a discussion of network neutrality avant la lettre in economic terms, see Eli Noam, *Beyond liberalization II: The impending doom of common carriage*, 18 TELECOMMUNICATIONS POLICY 435 (1994)

[12] James Speta, *A Sensible Next Step on Network Neutrality: The Market Power Question*, 8 REVIEW OF NETWORK ECONOMICS 113-127; Barbara Van Schewick, *Towards an Economic Framework for Network Neutrality Regulation, 5* JOURNAL ON TELECOMMUNICATIONS & HIGH TECHNOLOGY LAW 329-392 (2007); Tim Wu, *Network neutrality, broadband discrimination*, 2 JOURNAL ON TELECOMMUNICATIONS & HIGH TECHNOLOGY LAW 141 (2003); Christopher Yoo, *Beyond Network Neutrality*, 19 HARVARD

JOURNAL OF LAW AND TECHNOLOGY 2 (2005); Christopher Yoo,*Network neutrality and the economics of congestion*, 94 GEORGETOWN LAW JOURNAL 1849 (2006).

[13] B. E Hermalin & M. L Katz, *The economics of product-line restrictions with an application to the network neutrality debate*, 19 INFORMATION ECONOMICS AND POLICY 214-248 (2007); Florian Schuett, *Network Neutrality: A Survey of the Economic Literature*, 9 REVIEW OF NETWORK ECONOMICS (2010). For a discussion of network neutrality avant la lettre in economic terms, see Eli Noam, *Beyond liberalization II: The impending doom of common carriage*, 18 TELECOMMUNICATIONS POLICY 435 (1994)

[14] David Clark, *Network Neutrality: Words of Power and 800-Pound Gorillas*, 1 INTERNATIONAL JOURNAL OF COMMUNICATION 701-708 (2007); Jon M. Peha, The Benefits and Risks of Mandating Network Neutrality, and the Quest for a Balanced Policy, 1 INT'L J. COMM. 644, 644-659 (2007).

[15] See, e.g. FCC Report and Order, IN THE MATTER OF PRESERVING THE OPEN INTERNET AND BROADBAND INDUSTRY PRACTICES, GN DOCKET NO. 09-191, WC DOCKET NO. 07-52, FCC 10-201 § 21-30 (2010).

[16] See JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET, AND HOW TO STOP IT. (Yale University Press, 2008) for a detailed study on this trade-off.

[17] In the US this idea has led to the distinction between 'regular' Internet traffic and 'specialized services,' the latter requiring more network management because of their for instance time-sensitive nature. See FCC Report and Order (2010) at §112-114

[18] Some authors question the distinction between degrading and prioritising altogether, as they find that the latter naturally presupposes the former. See, e.g. Filomena Chirico, Ilse Van der Haar & Pierre Larouche,*Network Neutrality in the EU*, TILEC DISCUSSION PAPER (2007), http://ssrn.com/abstract=1018326

[19] J. Scott Marcus, *Network Neutrality: The Roots of the Debate in the United States*, 43 INTERECONOMICS 30-37 (2008).

[20] Jasper P. Sluijs, *Network Neutrality Between False Positives and False Negatives: Introducing a European Approach to American Broadband Markets*, 62 FEDERAL COMMUNICATIONS LAW JOURNAL 77-117 (2010); M. Cave & P. Crocioni, *Does Europe Need Network Neutrality Rules?*, 1 INTERNATIONAL JOURNAL OF COMMUNICATION 669–679 (2007); Peggy Valcke et al., *Guardian Night or Hands off? The European Response to Network Neutrality: Legal Considerations on the Electronic Communications Reform*, 72 COMMUNICATIONS & STRATEGIES 89-112 (2008);

[21] This is referred to as the EU regulatory framework for Electronic Communications, which is comprised of a set of six directives. For the last iteration, see DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 25 NOVEMBER 2009 AMENDING DIRECTIVES 2002/21/EC ON A COMMON REGULATORY FRAMEWORK FOR ELECTRONIC COMMUNICATIONS NETWORKS AND SERVICES, 2002/19/EC ON ACCESS TO, AND INTERCONNECTION OF, ELECTRONIC COMMUNICATIONS NETWORKS AND SERVICES, AND 2002/20/EC ON THE AUTHORISATION OF ELECTRONIC COMMUNICATIONS NETWORKS AND SERVICES., OJ L. 337/37 (2009); and 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, 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 CONSUMER PROTECTION COOPERATION, OJ L. 337/11 (2010).

[22] *Framework Directive* 2002/21/EC as amended. *id*, at rec. 5

[23] *Framework Directive* 2002/21/EC as amended *id*, at art. 8(5)(f): "[The national regulatory authorities shall impose] ex-ante regulatory obligations only where there is no effective and sustainable competition and relaxing or lifting such obligations as soon as that condition is fulfilled."

[24] See Pietro Crocioni, *Leveraging of Market Power in Emerging Markets: A Review of Cases, Literature, and a Suggested Framework*, 4 JOURNAL OF COMPETITION LAW AND ECONOMICS 449 (2008) and *Sluijs, Network Neutrality Between False Positives and False Negatives* (2010) for more information on the difficulties involved in regulating emerging markets such as broadband.

[25] European Commission, COMMISSION STAFF WORKING DOCUMENT: IMPACT ASSESSMENT SEC(2007) 1472 at 90-102 (2007)

[26] Universal Service Directive 2002/22/EC, as amended, art. 21(3)(d): ISPs can be required, amongst other things, to "provide information on any procedures put in place by the provider to measure and shape traffic so as to avoid filling or overfilling a network link, and on how those procedures could impact on service quality."

[27] See Jasper P. Sluijs, Florian Schuett & Bastian Henze, *Transparency regulation in broadband markets: Lessons from experimental research*, 35 TELECOMMUNICATIONS POLICY 592-602 (2011) for an experimental analysis of transparency regulation in broadband.

[28] We who have signed this open letter urge the European Parliament to protect the freedom to receive and distribute content, and to use services and applications without interference from private actors. We call on the Members of the Parliament to take decisive action during the ongoing negotiation of the Telecoms Package in order to guarantee a free, open and innovative Internet, and to safeguard the fundamental freedoms of European citizens. La Quadrature du Net, WE MUST PROTECT NET NEUTRALITY IN EUROPE! - OPEN LETTER TO THE EUROPEAN PARLIAMENT (2010), http://www.laquadrature.net/en/we-must-protect-net-neutrality-in-europe-open-letter-to-the-european-parliament.

[29] See, e.g. NN Squad Italia, QUESTIONNAIRE FOR THE PUBLIC CONSULTATION ON THE OPEN INTERNET AND NET NEUTRALITY IN EUROPE (2010),http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/net_neutrality/comments/index_en.htm ("There is another area of concern related to the technologies employed in the traffic management: in order for the operators to be able to manage traffic to some significant effectiveness, the payload of the sequences of data packets needs to be collected, reassembled and examined. Examining the headers or single packets is simply not effective. The widespread, uncontrolled deployment of Deep Packet Inspection technologies on operators' networks, absent any policy, can expose the user's traffic to privacy threats.").

[30] This was testified by the Parliament's infamous amendment 138 to the new Regulatory Framework for Electronic Communications, which nearly derailed the passing of the entire set of Directives: No restriction may be imposed on the fundamental rights and freedoms of end- users, without a prior ruling by the judicial authorities, notably in accordance with Article 11 of the Charter of Fundamental Rights of the European Union on freedom of expression and information, save when public security is threatened in which case the ruling may be subsequent. PARL. EUR. DOC. A6-0321/138 (2008).

[31] See, e.g. J. Cave et al. DOES IT HELP OR HINDER? PROMOTION OF INNOVATION ON THE INTERNET AND CITIZENS' RIGHT TO PRIVACY, Study for the European Parliament's Directorate General for Internal Policies, IP/A/ITRE/ST/2011-10 (Brussels, 2010).

[32] *Framework Directive* 2002/21/EC, as amended, art. 1.3.a Any of these measures regarding end-users' access to, or use of, services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms.

[33] BEREC, BEREC RESPONSE TO THE EUROPEAN COMMISSION'S CONSULTATION ON THE OPEN INTERNET AND NET NEUTRALITY IN EUROPE. BOR (10) 42 (2010),http://www.erg.eu.int/doc/berec/bor_10_42.pdf at 20 ("Freedom of expression and citizens rights, as well as media pluralism and cultural diversity, are important values of the modern society, and they are worth being protected in this context – especially since mass communication has become easier for all citizens thanks to the Internet However intervention in respect of such considerations lies outside the competence of BEREC, and we will not comment much on these issues, although it is noted that as public bodies, NRAs are obliged to respect the rights of citizens if restrictions are imposed on end users' access to or use of services.")

[34] *Framework Directive* 2002/21/EC, as amended, recital 29.

[35] "Filtering of Internet content is a threat to fundamental rights. Net neutrality is guaranteed. Within the network there are no restrictions on content, equipment or on the modes of communication allowed - while not degrading other traffic." Free Knowledge Institute, PUBLIC CONSULTATION ON THE OPEN INTERNET

AND NET NEUTRALITY IN EUROPE at 4 (2010),http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/net_neutrality/comments/index_en.htm.

[36] See, e.g. M. Ammori, *Beyond Content Neutrality: Understanding Content-Based Promotion of Democratic Speech*, 61 FEDERAL COMMUNICATIONS LAW JOURNAL 273 (2009); D. Kang, *Race. Net Neutrality*, 6 JOURNAL ON TELECOMMUNICATIONS & HIGH TECHNOLOGY LAW (2007); A. M Schejter & M. Yemini, *Justice, and only Justice, You Shall Pursue: Network Neutrality, the First Amendment and John Rawls's Theory of Justice,* 14 MICHIGAN TELECOMMUNICATIONS & TECHNOLOGY LAW REVIEW 137–457 (2007); Moran Yemini, *Mandated Network Neutrality and the First Amendment: Lessons from Turner and a New Approach*, 13 VIRGINIA JOURNAL OF LAW AND TECHNOLOGY 1 (2008); Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 UNIVERSITY OF ILLINOIS LAW REVIEW 1417; Dawn Nunziato, VIRTUAL FREEDOM: NET NEUTRALITY AND FREE SPEECH IN IHE INTERNET AGE (Stanford University Press, 2009).

[37] This is not to say that legal scholars in Europe have not related network neutrality issues to fundamental rights law, see e.g. CHRISTOPHER MARSDEN, NET NEUTRALITY: TOWARDS A CO-REGULATORY SOLUTION (Bloomsbury Academic Press, 2010). However, fundamental-rights research focusing specifically on network management seems to be lacking.

[38] STEVEN HICK, EDWARD F. HALPIN & ERIC HOSKINS, HUMAN RIGHTS AND THE INTERNET (2000)

[39] *Framework Directive* 2002/21/EC, as amended.

[40] See, e.g. Bits of Freedom & EDRI, RESPONSE OF BITS OF FREEDOM AND EDRI TO THE PUBLIC CONSULTATION OF THE EUROPEAN COMMISSION ON THE OPEN INTERNET AND NET NEUTRALITY IN EUROPE at 3 (2010), http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/net_neutrality/comments/index_en.htm. ("Thus, in the open internet, users can all freely communicate, fully express themselves, access information and participate in the public debate, without unneccessary [sic] interference by gatekeepers or middlemen. The end-to-end principle provides an important safeguard against censorship, both by public and private actors.")

[41] It should be noted that the Council of Europe, the institution behind the ECHR goes beyond the European Union to also include non-EU members such as Russia and Turkey. For a current index of High Contracting Parties, see http://www.coe.int/aboutCoe/index.asp?page=47pays1europe&l=en

[42] See Paul Lemmens, *The Relation between the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights - Substantive Aspects*, 1 MAASTRICHT JOURNAL OF EUROPEAN AND COMPARATIVE LAW 49 (2001) for a comparative analysis of the ECHR and the Charter.

[43] Art. 6(2) Treaty of the European Union (TEU). See Tobias Lock, *Accession of the EU to the ECHR: Who Would Be Responsible in Strasbourg?*, SSRN ELIBRARY (2010),http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1685785 for a critical analysis of the practicalities of EU ascension into the Convention.

[44] See, art. 21 TEU and art. 67(1) Treaty on the Functioning of the European Union (TFEU).

[45] See, e.g. La Quadrature du Net (2010).

[46] See, e.g. LIGUE ODEBI, CONSULTATION PUBLIQUE SUR L'INTERNET OUVERT ET LA NEUTRALITE DU NET: REPONSE DE LA LIGUE ODEBI AU QUESTIONNAIRE DE LA COMMISSION EUROPEENNE, 3 (2010), http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/net_neutrality/comments/index_en.htm. ("[E]n utilisant des procédés de Deep Packet Inspection (DPI), c'est à dire en ouvrant les paquets IP pour en lire le contenu. Cette inspection est très exactement analogue à l'ouverture d'une lettre par la poste : c'est un viol du secret des correspondances. Que ce dernier soit effectué par une machine ou par un humain n'y change rien: dans une démocratie, le contenu des communications échangées entre une source et un destinataire n'a pas à être lu par un postier ou un opérateur, dont le seul rôle est l'acheminement. Le secret des correspondances doit être respecté et clairement garanti par la loi, et si un doute persiste sur l'interprétation des textes existants quant à leur application à Internet, alors le législateur doit y remédier."—"Using Deep Packet Inspection (DPI) is like opening the IP packets to read the content. This inspection is exactly analogous to the postal service opening a letter: it is a violation of the secrecy of

correspondence. Whether this is done by a machine or a human makes no difference: in a democracy the content of communications between a sender and receiver may not be read by a postman or an operator, whose only role is the conveyance of mail. The confidentiality of correspondence should be respected and clearly guaranteed by law, and when there is doubt how to interpret existing laws when applied to the Internet, then the legislative branch must address this." [authors' translation])

[47] See, e.g. Cory Doctorow, DENIAL OF SERVICE, SIT-INS AND THE POLITICS OF THE CLOUD CORY DOCTOROW'S CRAPHOUND.COM (2011), http://craphound.com/?p=3577 discussing the similarities and differenced between sit-ins and Distributed Denial of Service (DDoS) Attacks .

[48] See, e.g. Michael Geist, TELUS BLOCKS SUBSCRIBER ACCESS TO UNION WEBSITE (2005), http://www.michaelgeist.ca/index.php?option=com_content&task=view&id=904&Itemid=85&nsub=.

[49] Jasper P. Sluijs, From Competition to Freedom of Expression: Introducing art. 10 ECHR in the European Network Neutrality Debate. TILEC Discussion Paper 2011-040, 2011, http://ssrn.com/abstract=1927814, forthcoming, Human Rights Law Review (2012)

[50] 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, OJ L 281/31 (1995)

[51] 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, OJ L 201/37 (2002)

[52] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC OJ L105/54 (2006)

[53] For an overview of the EU privacy and data-protection law instruments and their relation to network neutrality, see EDPS, Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data, 2011, http://ec.europa.eu/bepa/european-group-ethics/docs/activities/peter_hustinx_presentation_(1)_15_rt_2011.pdf.

[54] Peck v. The United Kingdom, app. 44647/98 (2003) at §57 ('Private life is a broad term not susceptible to exhaustive definition', which includes 'a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"').

[55] Copland v. The United Kingdom, app. 62617/00 (2007) at §43 ('e-mails sent from work should be (…) protected under Article 8, as should information derived from the monitoring of personal internet usage').

[56] T. De la Mare, B. Kennel &. C. Donnely, *Art. 8: Right to Respect for Family Life, Home and Correspondence*, HUMAN RIGHTS AND PRACTICE (Lester, Pannick & Herberg, eds.) (LexisNexis 2009) 359-452, 359.

[57] Société Colas Est et al. v. France, app. 37971/97 (2002) at §42.

[58] Wieser and Bicos Beteiligungen GmbH v. Austria, app. 74336/01 (2008) at §42-46

[59] De la Mare et al. (2009), at 396.

[60] See, e.g. Asselbourg et al. and Greenpeace v. Luxembourg, app. 29121/95 (1999) ("la Cour estime qu'une association non gouvernementale ne peut se prétendre victime d'une violation du droit au respect de son 'domicile,' au sens de l'article 8 de la Convention, (…) lorsque l'atteinte au droit au respect du domicile résulte, comme allégué en l'espèce, de nuisances ou de troubles qui ne peuvent être ressenties que par des personnes physiques."—"the Court considers that a non-governmental organization cannot claim to be a victim with respect to the right to privacy of one's 'home' within the meaning of Article 8 of the Convention (...) because an interference with the privacy of one's home, as alleged in this case, can result only in a nuisance or disorder experienced by physical persons" [authors' translation]).

[61] See, e.g. NN Squad Italia, QUESTIONNAIRE FOR THE PUBLIC CONSULTATION ON THE OPEN INTERNET AND NET NEUTRALITY IN EUROPE

(2010),http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/net_neutrality/comments/index_en.htm ("There is another area of concern related to the technologies employed in the traffic management: in order for the operators to be able to manage traffic to some significant effectiveness, the payload of the sequences of data packets needs to be collected, reassembled and examined. Examining the headers or single packets is simply not effective. The widespread, uncontrolled deployment of Deep Packet Inspection technologies on operators' networks, absent any policy, can expose the user's traffic to privacy threats.").

[62] INFORMATION TECHNOLOGY—OPEN SYSTEMS INTERCONNECTION—BASIC REFERENCE MODEL: CONVENTIONS FOR THE DEFINITION OF OSI SERVICES 12 (1993).

[63] Ralf Bendrath & Milton Mueller, *The End of the Net as We Know It? Deep Packet Inspection and Internet Governance*, SSRN ELIBRARY (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1653259.

[64] EDPS, Opinion on net neutrality (2010), at para. 32.

[65] Bendrath & Mueller (2010), at 5.

[66] I.M. Chettiar and J.S. Holladay, *Free to Invest. The Economic Benefits of Preserving Net Neutrality*, Institute for Policy Integrity, Report No. 4, 2010 at 19.

[67] Chris Marsden, Public Consultation On The Open Internet And Net Neutrality In Europe, http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/net_neutrality/comments/index_en.htm

[68] PAUL OHM, 'The Rise and Fall of Invasive ISP Surveillance', *University of Illinois Law Review* (2009) at 1468-69.

[69] Paul Ohm, 'The Rise and Fall of Invasive ISP Surveillance', *University of Illinois Law Review* (2009) at 1468 ('providers have begun examining much more information, and particularly content information, using automated, always-on DPI tools').

[70] See, e.g., Klass v. Germany, app. 5029/71 (1978) at §40-41 (any surveillance measure 'to open and inspect mail and post, to read telegraphic messages and to monitor and record telephone conversations (...) would result in an interference (…) with the exercise of that individual's right to respect for his private and family life and his correspondence'); Copland v. The United Kingdom, app. 62617/00 (2007) at §43 (art. 8(1) covers 'information derived from the monitoring of personal internet usage').

[71] The independent EU Advisory Body on Data Protection and Privacy, whose remit is defined under Article 30 of the EU Directive 95/46/EC and in Article 15 of EU Directive 2002/58/EC.

[72] ART. 29 WORKING PARTY, OPINION 1/2008 ON DATA PROTECTION ISSUES RELATED TO SEARCH ENGINES 8 (2008),http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf.

[73] Rotaru v. Romania, app. 28341/95 (2000); P.G. and J.H. v. The United Kingdom, app. 44787/98 (2001); see extensively PAUL DE HERT & SERGE GUTWIRTH, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalization in Action', in *Reinventing Data Protection?* (Serge Gutwirth, et al. eds., 2009).

[74] Malone v. The United Kingdom, app. 8691/79 (1984); P.G. and J.H. v. The United Kingdom, app. 44787/98 (2001).

[75] P.G. and J.H. v. The United Kingdom, app. 44787/98 (2001) at §42: 'The Court notes, however, that metering (…) does not per se offend against Article 8 if, for example, done by the telephone company for billing purposes'.

[76] Malone v. The United Kingdom, app. 8691/79 (1984) at §84.

[77] Copland v. The United Kingdom, app. 62617/00 (2007) at §43.

[78] Copland v. The United Kingdom, app. 62617/00 (2007) at §44 ('the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference').

[79] J.C. FISCHER, *Communications Network Traffic Data. Technical and Legal Aspects*, PhD Thesis Eindhoven University of Technology, Eindhoven 2010, at 26, 30-31.

[80] This service type subdivision is analogous to the distinction the eCommerce Directive makes in terms of liability for ISP or other intermediaries, see 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 178/1 (2000), art. 12-14.

[81] Fischer (2010), at 214.

[82] Fischer (2010), at 30.

[83] Rees v. The United Kingdom, app. 9532/81 (1986) at §47 ('The Convention has always to be interpreted and applied in the light of current circumstances (…). The need for appropriate legal measures should therefore be kept under review having regard particularly to scientific and societal developments').

[84] Peck v. The United Kingdom, app. 44647/98 (2003) at §57.

[85] X v. Federal Republic of Germany, app. 2375/64 (1967).

[86] Pieter Van Dijk, *Right to Respect for Privacy (Article 8), in* THEORY AND PRACTICE OF THE *European Convention of Human Rights* , 730 (Pieter Van Dijk et al. eds., 2006).

[87] Golder v. The United Kingdom, app. 4451/70 (1975); De Wilde, Ooms and Versyp v. Belgium ("Vagrancy"), app. 2832/66; 2835/66; 2899/66 (1971).

[88] Golder v. The United Kingdom, app. 4451/70 (1975); Silver and others v. The United Kingdom, app. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 (1983).

[89] See the section on 'Non-DPI-based degrading or prioritising traffic' above.

[90] YOCHAI BENKLER ET AL., NEXT GENERATION CONNECTIVITY: A REVIEW OF BROADBAND INTERNET TRANSITIONS AND POLICY FROM AROUND THE WORLD at 308 (2010).

[91] *See, e.g.* Bergens Tidende and Others v. Norway, app. 26132/95 (2000). *and* Fuentes Bobo v. Spain, app. 39293/98 (2000).

[92] See Powell and Rayner v. the United Kingdom, app. 9310/81, 41 (1990) ("Whether the present case be analysed in terms of a positive duty on the State to take reasonable and appropriate measures to secure the applicants' rights under paragraph 1 of Article 8 (art. 8-1) or in terms of an "interference by a public authority" to be justified in accordance with paragraph 2 (art. 8-2), the applicable principles are broadly similar.").

[93] A case in point is the French *Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet* [Law to promote the dissemination and protection of creativity on the Internet, also referred to as HADOPI Act], *Journal Officiel* 135 of 13 June 2009 (consolidated version 30 October 2009) (inserting art. L336-3 Intellectual Property Code, which obliges ISPs to monitor that subscribers do not infringe copyright or neighbouring rights law).

[94] Cf. art. 22(3) of the Universal Service Directive 2002/22/EC, as amended, stipulating that regulatory authorities should be able to set minimum quality-of-service standards ('In order to prevent the degradation of service and the hindering or slowing down of traffic over networks, Member States shall ensure that national regulatory authorities are able to set minimum quality of service requirements').

[95] Directive 2002/21/EC, as amended.

[96] BASIE VON SOLMS, 'Information Security – The Fourth Wave', *25 Computers & Security* (2006) at 166 ('Information Security is and has always been the discipline to mitigate risks impacting on the confidentiality, integrity and availability of (...) IT resources').

[97] See art. 4 of the French Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2) (allowing administrative authorities to order blocking of websites containing evident child-pornographic content); German Zugangserschwerungsgesetz [Access Impediment Act] (obliging larger access providers to block access to blacklisted child-pornographic websites). Note that the German law is in force since 2010 but is not enforced and will be withdrawn. See, generally, European Digital Rights, *Internet blocking*, http://www.edri.org/taxonomy/term/44 (last accessed 21 April 2011).

[98] E.g., Danish Supreme Court 27 May 2010, case 153/2009 (obliging Telenor to block access to The Pirate Bay); SABAM v. S.a. Tiscali (Scarlet) District Court of Brussels, no. 04/8975/a, 29 June 2007 (Court order requiring an ISP to filter traffic in order to detect copyright infringement); British High Court, 20th

Century Fox et al. v BT [2011] EWHC 1981 (Ch) (Court order requiring BT to block copyright infringing usenet site).

[99] See, e.g., Belgian Commercial Court Antwerp 9 July 2010; Dutch District Court The Hague 19 July 2010, LJN BN1445; Irish High Court 11 October 2010, EMI and Others v. UPC, all rejecting plaintiff's motion to oblige ISPs to block access to The Pirate Bay.

[100] See, e.g., 'Telenor and KRIPOS introduce Internet child pornography filter', http://presse.telenor.no/PR/200409/961319_5.html (last accessed 21 April 2011).

[101] M.M. v. the Netherlands, app. 39339/98 at §39.

[102] See, e.g., Digital Rights Ireland, 'FOI shows Department of Justice planning internet blocking for Ireland', 16 April 2010, http://www.digitalrights.ie/2010/04/16/foi-shows-department-of-justice-planning-internet-blocking-for-ireland/ (last accessed 21 April 2011).

[103] See, e.g. Universal Service Directive 2002/22/EC, as amended, at art. 20.

[104] However, such behavior by ISPs may prompt States such as the Netherlands to recognize positive obligations in these matters and impose regulation to prevent such behavior. See Kevin O'brien, *Dutch Lawmakers Adopt Net Neutrality Law*, THE NEW YORK TIMES, June 22, 2011, http://www.nytimes.com/2011/06/23/technology/23neutral.html&hpw.

[105] See Powell and Rayner v. the United Kingdom, app. 9310/81, 41 (1990).

[106] See JEAN-FRANÇOIS AKANDJI-KOMBE, POSITIVE OBLIGATIONS UNDER THE EUROPEAN CONVENTION ON HUMAN RIGHTS: A GUIDE TO THE IMPLEMENTATION OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS (Council of Europe 2007) on recent ECHR case law involving positive obligations.

[107] Novoseletskiy v. Ukraine, app. 47148/99 (2005).

[108] E.g., Marckx v. Belgium, app. 6833/74 (1979); X. and Y. v. the Netherlands, app. 8978/80 (1985); Hatton and others v. The United Kingdom, app. 36022/97 (2003).

[109] *See, e.g.* Cotlet v. Romania, app. 38565/97 (2003) at §57 ("La Cour note que le requérant se plaint en substance non pas d'un acte, mais de l'inaction de l'Etat. Elle rappelle à cet égard que, si l'article 8 a essentiellement pour objet de prémunir l'individu contre les ingérences arbitraires des pouvoirs publics, il ne se contente pas de commander à l'Etat de s'abstenir de pareilles ingérences: à cet engagement négatif peuvent s'ajouter des obligations positives inhérentes à un respect effectif des droits gratis par l'article 8 précité"—"The Court notes that the applicant did not substantially complain about the actions, but about the inaction of the State. The Court recalls in this respect that, if Article 8 is essentially designed to protect the individual against arbitrary interference by public authorities, it does not merely order the State to abstain from such interference: this negative right can carry positive obligations inherent to the effective protection of the rights enshrined in Article 8 cited above." [authors' translation]).

[110] K.U. v. Finland, app. 2872/02 (2008).

[111] Jonathan Zittrain & John Palfrey, 'Internet Filtering: The Politics and Mechanisms of Control', in *Access Denied. The Practice and Policy of Global Internet Filtering* (Ronald Deibert, et al. eds., 2008) at 35 (referring to 'the overblocking or underblocking that is today inherent in any filtering regime').

[112] Cf. Dudgeon v. Ireland, app. 7525/76 (1981) (recognizing sexual life as part of private life), Norris v. Ireland, app. 10581/83 (1988) (finding an interference in case sexual life is continuously and directly affected), and Goodwin v. The United Kingdom, app. 28957/95 (2002) (assuming positive obligations to legally recognize transsexuality).

[113] Stjerna v. Finland, app. 18131/91, §38 (1994) ("The boundaries between the State's positive and negative obligations under Article 8 (art. 8) do not lend themselves to precise definition. (…) [R]egard must be had to the fair balance that has to be struck between the competing interests of the individual and of the community as a whole").

[114] Cotlet v. Romania, app. 38565/97 (2003) at §58

[115] López-Ostra v. Spain, app. 16798/90, §51 (1994).

[116] Van Dijk, *Right to Respect for Privacy* (2006), at 745.

[117] Cf. art. 4 of the French LOPPSI 2, discussed above.

[118] Cf. Danish Supreme Court 27 May 2010 and other cases discussed above.

[119] Malone v. The United Kingdom, app. 8691/79 (1984); Kruslin v. France, app. 11801/85 (1990) and Huvig v. France, app. 11105/84 (1990).

[120] Poltoratskiy v. Ukraine, app. 38812/97 (2003).

[121] Kruslin v. France, app. 11801/85 (1990) at §33, Huvig v. France, app. 11105/84 (1990) at §32 (italics added).

[122] Danish Supreme Court 27 May 2010, case 153/2009, available at http://www.domstol.dk/hojesteret/Documents/Domme/153-09.pdf (last accessed 21 April 2011).

[123] Danish Supreme Court 27 May 2010, case 153/2009, p. 5 (our translation).

[124] Herczegfalvy v. Austria, app. 10533/83 (1992) at §91.

[125] Kruslin v. France, app. 11801/85 (1990) at §27, Huvig v. France, app. 11105/84 (1990) at §26.

[126] 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, OJ L178/1 (2000)

[127] Herczegfalvy v. Austria, app. 10533/83 (1992) at §91.

[128] See *Framework Directive* 2002/21/EC, as amended.

[129] See, for instance, the German Telecommunications Act (Telekommunikationsgesetz), at §109(2): Wer Telekommunikationsanlagen betreibt, die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen, hat darüber hinaus bei den zu diesem Zwecke betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, und gegen äußere Angriffe und Einwirkungen von Katastrophen zu treffen. ("He who operates telecommunications facilities that provide telecommunications services to the public, shall furthermore, in the operation of telecommunications and data-processing systems for these purposes, have implemented technical or other measures to protect against disruptions that lead to significant impairments of telecommunications networks, and against external attacks or effects of natural disasters" [authors' translation]).

[130] Yutaka Arai, *The System of Restrictions*, in THEORY AND PRACTICE OF THE *European Convention of Human Rights* 333-350, 340 (Pieter Van Dijk et al. eds., Fourth ed. 2006).

[131] Kamma v. Netherlands, app. 4771/71, Commission Report (1974) ("There may, however, be a violation of Art. 18 in connection with another Article, although there is no violation of that Article alone").

[132] M. Granger Morgan & Elaine Newton, 'Protecting Public Anonymity', *21 Issues in Science and Technology* (2004) (describing function creep as follows: "Once a system has been developed with a rich set of capabilities, inventive people often can find other important, beneficial but perhaps also pernicious ways to use it.")

[133] Van Dijk, *Right to Respect for Privacy* (2006), at 750.

[134] Golder v. The United Kingdom, app. 4451/70 (1975) at §45 ('The "prevention of disorder or crime", for example, may justify wider measures of interference in the case of such a prisoner than in that of a person at liberty').

[135] Golder v. The United Kingdom, app. 4451/70 (1975) at §45 ('The Court again lays stress on the fact that Golder was seeking to exculpate himself of a charge (…). In these circumstances, Golder could justifiably wish to write to a solicitor'); see also, e.g., Schönenberger and Durmaz v. Switzerland, app. 11368/85 (1988), Herczegfalvy v. Austria, app. 10533/83 (1992).

[136] Cf. Herczegfalvy v. Austria, app. 10533/83 (1992) at §91 ('such specifications appear all the more necessary in the field of detention in psychiatric institutions in that the persons concerned are frequently at the mercy of the medical authorities, so that their correspondence is their only contact with the outside world').

[137] Poltoratskiy v. Ukraine, app. 38812/97 (2003).

[138] Jonathan Zittrain & John Palfrey, 'Internet Filtering: The Politics and Mechanisms of Control', in *Access Denied. The Practice and Policy of Global Internet Filtering* (Ronald Deibert, et al. eds., 2008), 29-56.

[139] Cf. Silver and others v. The United Kingdom, app. 5947/72 (1983) at §105, finding that letters containing threats of violence or discussing other criminals were legitimately blocked, while the blocking of letters on many other grounds was a violation of art. 8.

[140] Cf. Pfeifer and Plankl v. Austria, app. 10802/84 (1992) at §47, finding that the deletion of passages in letters with "jokes of an insulting nature against prison officers", similarly to Silver's private letters "calculated to hold the authorities up to contempt", was disproportionate.

[141] Cf. the opinion of the Advocate General in CoJ-EU Case C-70/10 (Scarlet Extended v. Société belge des auteurs compositeurs et éditeurs (Sabam)), arguing that 'EU law precludes a national court from making an order, on the basis of the Belgian statutory provision, requiring an internet service provider to install, in respect of all its customers, in abstracto and as a preventive measure, entirely at the expense of the internet service provider and for an unlimited period, a system for filtering all electronic communications passing via its services (in particular, those involving the use of peer-to-peer software) in order to identify on its network the sharing of electronic files containing a musical, cinematographic or audio-visual work in respect of which a third party claims rights, and subsequently to block the transfer of such files'. See Press Release No. 37/11 of 14 April 2011,http://europa.eu/rapid/pressReleasesAction.do?reference=CJE/11/37&type=HTML (last accessed 4 May 2011).

[142] CoJ-EU Case C-70/10 (Scarlet Extended v. Sabam).

[143] Cf. Pfeifer and Plankl v. Austria, app. 10802/84 (1992) at §47 ('The deletion of passages is admittedly a less serious interference' than the stopping of entire letters).

[144] Silver and others v. The United Kingdom, app. 5947/72.

[145] Copland v. The United Kingdom, app. 62617/00 (2007).