COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Steering Committee on Media and Information Society (CDMSI)

5th meeting
Strasbourg 3-6 December 2013

CDMSI(2013)misc19E

Protecting Human Rights through Network Neutrality: Furthering Internet Users' Interest, Modernising Human Rights and Safeguarding the Open Internet

"Providing guidance to member states and/or to facilitating the elaboration of guidelines with and for private sector actors in order to define more precisely acceptable management measures and minimum quality-of-service requirements"
(CM Declaration on Network Neutrality of 2010)

by

Luca Belli
Matthijs van Bergen[1]

---

1 The opinions expressed in this work are the responsibility of the author and do not necessarily reflect the official policy of the Council of Europe

Luca Belli is the founder and co-coordinator of the Dynamic Coalition on Network Neutrality of the United Nations Internet Governance Forum. Over the last three years, Mr Belli has cooperated with the Secretariat of the United Nations Internet Governance Forum, the Council of Europe Internet Governance Unit and with the Internet Society. Mr Belli is currently serving as a Council of Europe Expert on Network Neutrality and is completing his Doctoral Research in Public Law at Centre d'Etudes et de Recherches de Sciences Administratives et Politiques (CERSA), Université Panthéon-Assas (PRES Sorbonne University), Paris. Furthermore, Mr Belli is a former Internet Society Ambassador to the Internet Governance Forum and an alumnus of the Internet Society Next Generation Leaders Programme. Lastly, he is a senior author and a member of the steering committee of Medialaws.eu.

Matthijs van Bergen works as a legal advisor at ICTRecht, and is simultaneously developing his PhD thesis concerning net neutrality and the protection of freedom of speech and privacy in information societies at Leiden University. Matthijs has advised the Dutch NGO Bits of Freedom concerning net neutrality from 2010 to 2012, on an entirely voluntary ('pro bono') basis. Currently Matthijs is alsoserving as a network neutrality expert for the Council of Europe.

Foreword

1. Today's information societies co-exist in Cyberspace. As information and communication technologies and the Internet are becoming ever more omnipresent and essential for individuals' everyday activities, the technological architecture and design choices embedded in them, have ever greater consequences.

2. Most of the roughly 2,5 billion people currently connected to the Internet have come to rely on it as an essential tool to participate in democratic, economic and social life. Since access to the Internet has gone mobile, people's everyday use of the Internet is no longer limited to personal computers at home or at work and an increasing percentage of the European population is now connected 24x7 in a ubiquitous fashion. In all likelihood, the laptops, tablets and smartphones we carry to connect us on the go, will soon be supplemented, or even replaced, by glasses, watches and a plethora of other upcoming devices which will continually enable us to capture, communicate and enhance our realities through digital information processing and sharing. Our connection to and through the Internet is thus growing ever further towards a man-computer symbiosis.[2]

3. If information forms the "oxygen of the modern age", then the Internet may rightfully be regarded as modern humanity's respiratory system. In a similar manner as the bronchial tubes transport oxygen into the blood stream through many interconnections and branches, the Internet transports information, ideas and services between people all over the world through a web of interconnected networks. Data packets delivering information through the Internet are indeed becoming as vital as red blood cells, which deliver oxygen to the various body tissues. Therefore, it is crucial that Internet traffic, just as the blood stream, be managed in a sustainable fashion and in harmony with the constitutional requirements of the overall system. Hence, it must be ensured that fundamental principles of democratic systems such as the respect for human rights and pluralism, the separation of powers doctrine and the principle of subsidiarity, which have been at the heart of both European democracies and the Internet's initial development, continue to be play a fundamental role in the Internet's architecture, administration and management.

---

[2] According to Licklider in 1960, a "Man-computer symbiosis is an expected development in cooperative interaction between men and electronic computers." See Licklider J.C.R., IRE Transactions on Human Factors in Electronics, volume HFE-1, pages 4-11, March 1960.

4. Each democratic state therefore holds a responsibility of utmost importance, to ensure that the Internet remains a platform for democratic engagement and constitutional freedom, and does not evolve into an instrument of centralised control for both state and non-state actors[3].

[3] To this extent, see: McNamee J., *The Slide from "Self-regulation" to Corporate Censorship*, 2011.

Executive summary

5. This report was drafted with the goals to (i) provide deeper insight into how net(work) neutrality relates to human rights and (ii) suggest a policy and legal approach aimed at granting the full enjoyment of Internet users' fundamental rights and freedoms through an open and neutral Internet environment, while simultaneously promoting unrestrained innovation and economic growth in the digital economy.[4]

Network neutrality is a key enabler of human rights

6. Network neutrality prescribes that Internet traffic shall be treated without undue discrimination, restriction or interference, so that end-users[5] enjoy the "greatest possible access to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice".[6]

7. On the one hand, network neutrality is instrumental to enable any Internet user to offer and enjoy online content, applications and services through any Internet-connected device of their choice, without having to conclude agreements with each Internet Service Provider ("ISP") [7] of each intended recipient, and all ISPs in between. On the other hand, net neutrality ensures that Internet-users' choices for certain online content, applications, services and devices are not unduly influenced by discriminatory delivery of Internet traffic. As such, net neutrality enables self-determination and facilitates the openness of the Internet, by deflating market and institutional barriers to enter into the 'free market of ideas' and to participate on equal footing in economic, social and political activities.

---

4 With respect to the goals of this report, it should be noted that a number of participants to the Council of Europe Multi-Stakeholder Dialogue on Network Neutrality and Human Rights – a conference organised by the Council of Europe on 29-30 May 2013 – highlighted the interest of a policy framework aimed at safeguarding net neutrality. See: Belli L., Council of Europe Multi-Stakeholder Dialogue on Network Neutrality and Human Rights, Outcome Paper, June 2013. The concerns expressed during this conference led the Council of Europe to commission this report.

5 In this report we speak of Internet (or end-) users rather than consumers. This in order to reflect the idea that consumers are solely or primarily economic actors in a market setting, whereas 'Internet users' should be regarded as autonomous participants of an 'information society', connected through the Internet, with interests that range beyond the merely economical, including also social, political and other interests.

6 Council of Europe, 2010, Declaration of the Committee of Ministers on Network Neutrality, para. 4.

7 The term "Internet service provider" (ISP) is used to denote a legal person providing Internet connectivity to its customers. The term ISP also encompasses Internet transit providers – i.e. those entities that provide connectivity to various ISP, allowing them to interconnect their networks – but in this report, it does not include hosting providers and providers of online services, applications and content.

8. In our current information society, the ability to freely receive and impart ideas and information and to fully participate in democratic life is truly reliant on the nature of one's Internet connection.[8] By ascribing to users the ability to choose freely how to utilise their Internet connection, without undue interferences from public or private entities, network neutrality directly contributes to the effective enjoyment of a range of fundamental rights, such as Internet users' freedom of speech and right to privacy,[9] as well as the promotion of a diverse and pluralistic media-landscape, while unleashing a virtuous cycle of innovation without permission.

9. For such reasons the Committee of Ministers of the Council of Europe adopted the 2010 Declaration on network neutrality, underlining its commitment to this fundamental principle,[10] while in 2012 the Internet Governance Strategy of the Council of Europe urged the development of "human rights policy principles on "network neutrality" to ensure Internet users have the greatest possible access to content, applications and services of their choice as part of the public service value of the Internet and in full respect of fundamental rights"[11].

Network neutrality has come under threat

10. Certain Internet traffic management ("ITM")[12] techniques currently allow ISPs to block, downgrade or prioritise specific data flows. Research has shown that ITM is frequently deployed in order to block or downgrade specific Internet traffic relating to online services which compete with other services offered by the ISPs.[13] Such practices compromise end-users' capacity to freely receive and impart information online using applications, services and devices of their choice, and jeopardise the open and neutral character of Internet architecture. Furthermore, some large European ISPs have made clear through the media and other avenues, such as shareholders' meetings and industry associations, that they intend to depart from neutral Internet access provision, in order to

---

8 See: Council of Europe, Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet.

9 Some even suggest a notion of net neutrality as a human networking right sui generis. See: Berners Lee T., Long live the web, Scientific American 22 November 2010; https://en.wikipedia.org/wiki/Tim_Berners-Lee.

10 See: Council of Europe, 2010 Declaration of the Committee of Ministers on Network Neutrality, para 9, which also suggests further exploring network neutrality "within a Council of Europe framework with a view to providing guidance to member states". This suggestion has been reiterated by several participants to the Multi-Stakeholder Dialogue on Network Neutrality and Human Rights. See: Belli L., Council of Europe Multi-Stakeholder Dialogue on Network Neutrality and Human Rights, Outcome Paper, op.cit.

11 See: Council of Europe *Internet Governance, Council of Europe Strategy 2012-2015*, CM(2011)175 final, 15 March 2012, paragraph I.8.e.

12 According to BEREC ITM is: "all technical means used to process through the network traffic sent or received by end users, including both application-specific and application-agnostic traffic management. BEREC, A view of traffic management and other practices resulting in restrictions to the open Internet in Europe, 29 May 2012, p. 4.

13 Relating to Europe, see: BEREC, op. cit. Relating to the USA, see: FCC 10-201, Report and order on the open Internet 2010, paragraph 14.

discriminate and prioritise specific data-flows and monetise the value that specific online applications, services and content (conceived by Internet users) present to their subscribers.[14]

11. This illustrates that existing European approaches based purely on economic and competition-law principles have thus far failed to fully enforce the network neutrality principle, even though European telecommunications markets have generally been considered relatively competitive.[15] Indeed, just as the right to vote alone is not enough to ensure freedom in a constitutional democracy, the possibility to switch providers – which may be seen as the right to 'vote (an ISP) with your feet' – is not enough to adequately ensure the enjoyment of users' freedoms on the Internet.

12. Therefore, it seems necessary to query what kind of policy and legal approach would be best suited to enforce the network neutrality principle and safeguard the public-service value of the Internet.

A recommended policy and legal approach to network neutrality

13. In this report we propose a model framework on network neutrality which all Council of Europe member states can adopt in their legal systems. Importantly, the framework is directly inspired by article 10 ECHR, which ensures the right to receive and impart ideas and information without restriction or interference, unless such interference is strictly necessary for and proportionate to a legitimate aim. Since the goal is to ensure that Internet traffic shall be transmitted without undue discrimination, restriction or interference, whether by public or private actors, the format of article 10 ECHR lends itself very well to be transposed into a legal framework guaranteeing network neutrality.

---

[14] E.g. KPN Investor Day, London 10 May 2011; ETNO paper on Contribution to WCIT ITRs Proposal to Address New Internet Ecosystem.In response, see e.g.: BEREC, BEREC's comments on the ETNO proposal for ITU/WCIT or similar initiatives along these lines, BoR (12) 120 rev.1, 14 November 2012.

[15] It should be stressed that, at the EU level, the Universal Service Directive (i.e. directive 2002/22/EC) has strengthened consumer protection, fostering better consumer information pertaining to supply conditions and tariffs in order to allow them to more easily switch providers, thus promoting competition in the electronic communications markets. However, as pointed out by BEREC, several types of discriminatory practices are particularly widespread at the European level. See: BEREC, A view of traffic management and other practices resulting in restrictions to the open Internet, op. cit. Furthermore, it has been noted by the Netherlands Bureau for Economic Policy Analysis that "one cannot be optimistic about the intensity of competition [in the telecoms sector]. Moreover, if providers make their networks "less neutral" by implementing network bias practices, the intensity of competition decreases further. "See: CPB response of 23 September 2010 to the public consultation on Internet and net neutrality.

Table of Contents

I. The open Internet and network neutrality

"The global success of the Internet is owed to the fact that it is open, non-discriminatory and easily accessible. The maintenance of the structure requires the progressive development of international standards that are mutually recognised by states, the private sector, civil society and other relevant technical communities."

The Council of Europe, Internet Governance Strategy 2012-2015

14. As several scholars and competent authorities have argued, what makes the Internet an unquestionable innovation-galvaniser as well as a disruptive propellant of freedom of expression is its underlying open architecture.[16] The idea is that having fewer barriers and "gatekeepers" involved in the telecommunication process between end-points on a network, stimulates the free flow of information and the circulation of innovation, enabling freedom of expression. Openness achieves this by deflating both market and institutional barriers that could impede the participation of any interested stakeholder to a specific Internet-related activity, be it economic, social or political.

15. On the other hand, the concept of network neutrality refers to the regulatory strategy aimed at framing network management practices, so that openness can be safeguarded. By prescribing that Internet traffic shall be treated without undue discrimination, restriction or interference, network neutrality enables anyone to access and use all lawful online content, applications, services and devices as well as to offer them to all Internet users at once, without having to conclude any further agreement with the ISP of the recipient or with any ISPs in between, besides their own Internet access service contract. At the same time, net neutrality ensures that Internet-users' choices for certain online content, applications, services and devices are not unduly influenced by discriminatory traffic delivery.

16. As such, net neutrality facilitates the openness of the Internet, deflating barriers to enter into the 'free market of ideas' and to participate on equal footing in economic, social and political life. Indeed, network neutrality ensures that not only content which aligns with the (commercial) interests of ISPs is transmitted (with sufficient quality), but that all packets can count on a 'best-effort' delivery,

---

[16] For instance, see: Berkman Center for Internet & Society at Harvard Law School, Roadmap for Open ICT Ecosystems, 2005,; Kahin B. & Keller J., Public Access to the Internet, MIT Press, 1995; OECD, Communiqué on Principles for Internet Policy-Making, 28-29 June 2011; Van Schewick B., Internet Architecture and Innovation, MIT Press, 2010; Benkler Y., The Wealth of Networks, Yale University Press, 2006; Zittrain J., The Future of the Internet and How to Stop It, Yale University Press, 2008; FCC 10-201, report and order on the open Internet 2010; BEREC 2012, 'Overview of BEREC's approach to net neutrality', BoR (12) 140, 27 November 2012.

so that end-users truly enjoy "the greatest possible access to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice"[17].

17. Furthermore, network neutrality proves beneficial also with regard to end-users' privacy, because if ISPs cannot discriminate traffic for commercial purposes, they do not have a commercial interest in the inspection of the data-packets they deliver. If ISPs were to change their business model to gain a commercial interest in the type of content, services, applications and devices used by their customers, and discriminated their delivery quality accordingly, ISPs would naturally have to monitor users' behaviour, and try to influence it to maximise profits.

18. It is important to note that both net neutrality and openness facilitate inclusion, transparency, fair competition and non-discrimination with the goal of fostering participation, cooperative creativity and the full enjoyment of human rights. However, openness is a more overarching concept, the achievement of which is facilitated by the management of Internet traffic without undue discrimination, restriction or interference. Therefore, if the ultimate goal is to foster and safeguard openness by removing barriers, then the absence of undue discrimination in the network vis-à-vis online services, applications, content and devices, is essential to achieve this objective.

19. This reflection shows that, although network neutrality and openness are frequently regarded as interchangeable concepts, they are not entirely synonymous. These concepts align in that they are both reinforced by the "end-to-end principle"[18] and ultimately facilitate a free flow of information and innovation without discriminatory barriers. They diverge, however, in that openness is a broader concept alluding to an absence of barriers in general while neutrality primarily implies an absence of undue discrimination in the network-management sphere.

20. Besides net neutrality, the very processes by which technical Internet standards are elaborated[19] and Internet-related policy should be made[20] are also crucial components of the

---

17 See: Declaration by the Committee of Ministers on Internet governance principles, Adopted by the Committee of Ministers on 21 September 2011at the 1121st meeting of the Ministers' Deputies.

18 The end-to-end principle is a fundamental technical design principle, which is argued to have governed the Internet architecture since its inception. See: Jerome H. Saltzer, David P. Reed & David D. Clark, "End-to-end arguments in system design", in ACM Transactions on Computer Systems n°2, 1984; Network Working Group, Architectural Principles of the Internet, Request for Comments: 1958, June 1996; Network Working Group, The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture, Request for Comments: 3724, March 2004.

19 See: Internet Architecture Board, Affirmation of the Modern Paradigm for Standards, Request for Comments: 6852, January 2013.

20 To this extent, see: Council of Europe, Declaration by the Committee of Ministers on Internet governance principles, op. cit; OECD, Communiqué on Principles for Internet Policy-Making, op. cit. p. 4. .

openness of the Internet ecosystem. Indeed, to achieve the desired level of openness, it is of paramount importance that Internet standards and policies are crafted by open communities, through a collaborative effort, which remove barriers relating to participation, thus allowing all voices concerning any discussed matter to be heard on an equal footing[21]. Consequently, such an open approach is mirrored in the protocols and procedures defined by the Internet standards that remove market barriers and foster connectivity, thus allowing any end-user to build innovation on accessible technical specifications and to circulate their developments globally. In like manner, open Internet policy-making processes aim to remove institutional barriers, thus allowing every interested stakeholder to provide inputs and contribute to the elaboration of Internet-related policies in a transparent manner.

21. Furthermore, it should be highlighted that the edges-empowering architecture of the Internet, following from the end-to-end principle, plays a crucial role with regard to the achievement of an open Internet. By requiring that functionalities be implemented at the edges (hosts) when possible and at the core (routers) only when necessary, the end-to-end principle recalls the principle of subsidiarity[22] and places the end-users in control of their communications, allowing them to exercise their fundamental rights and freedoms and take informed decisions.[23] With respect to network neutrality, the end-to-end argument suggests that ISPs' interference by means of network management[24] be limited, and it prescribes that any potential discrimination in the transmission quality and priority of online content, applications, devices and services, shall be in direct control of the end-users.[25]

---

21 To this latter extent, see : Belli L. & Van Bergen M., "A Discourse-Principle Approach to Network Neutrality: A Model Framework and its Application", in Belli L. & DeFilippi P. (ed.), *The Value of Network Neutrality for the Internet of Tomorrow*, *Report of the Dynamic Coalition on Network Neutrality*, 2013.

22 The "broad version" of the end-to-end principle is defined by Barbara van Schewick as follows: "a function or service should be carried out within network layer [i.e., available to all clients of the network] only if it is needed by all clients of that layer." Art. 5(3) of the Treaty on the EU states: "Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level. The idea that the network serves the edges, also recalls the idea that democratic governments are there to serve its citizens. This implies that ISPs must respect the end users' human rights and fundamental freedoms.

23 See: Declaration by the Committee of Ministers on Internet governance principles *op. cit*.

24 For clarity, "in the network" here primarily refers to how functionality is distributed in a layered network architecture and less to the actual geographical location or legal ownership of the equipment. E.g. an e-mail server can be owned by an ISP and located in its premises, but in an architectural sense, an e-mail server is located at the edge of the network and not in the network. See Van Schewick B., 2010, *op. cit*. p. 67, p. 100 and p. 109-110.

25 It should be stressed that from the perspective of the end-to-end principle the imposition to an end-user of discriminatory treatment of certain types of is highly undesirable. See: Network Working Group, *Request for Comments: 1958, Architectural Principles of the Internet*, June 1996. To the extent that this is possible to implement, it would be more consistent with the end-to-end argument to provide to Internet-users the responsibility and means to set their own desired parameters for traffic management, *e.g*. via the configuration settings of their personal routers. Furthermore, as highlighted by Frode Sørensen, every device connected to the Internet can utilise 'congestion control'

22. Therefore, openness can be considered as both the conceptual basis and the ultimate goal of network neutrality. In fact, network neutrality stems from the original barrier-free, end-to-end design of the open Internet[26] and, simultaneously, should be considered as a key vector through which transparency, fair competition, and non-discrimination can come to be, thus making the Internet open. Both Internet openness and network neutrality are therefore particularly beneficial to the effective enjoyment of Internet-users' fundamental rights. Consequently, network neutrality is considered both as a "policy priority"[27] as well as a fundamental "network design principle"[28] guiding the implementation of the openness principle into the network-management context.

23. In fact, it seems important to underline that although openness seems fairly conceptually clear on the surface, its multifaceted nature lends itself to potentially diverging interpretations, in a similar manner as other "essentially contested concepts", such as of 'freedom' and 'democracy'.[29] In this respect, it should also be noted that analogous to the concepts of freedom and democracy, the idea of openness is particularly useful to provide a general vision towards which public policies can be orientated, but its internal complexity demands the utilisation of instrumental principles, such as the network neutrality principle, in order to be implemented.

---

software that constantly "downgrades more or less all types of traffic whenever there is any sign of congestion in the network. This type of 'downgrading' is implemented based on the end-to-end principle, and the functionality is called 'congestion control'. When our Internet-connected computers 'at the edge' are pumping IP-packets, they will automatically back off when they discover that packet(s) get lost (which usually happens because of lack of capacity in some router out there on the Internet). [...] Therefore it is debated to what extent, and in what way, the network (i.e. the routers and similar network-internal equipment) actually need to assist this congestion mitigation, since this is already handled at the edge, in the endpoints. Such an 'assistance' in the core is often referred to as 'congestion management' to distinguish it from 'congestion control'". See: Sørensen F., Reply to the mailing-list of the Dynamic Coalition on Network Neutrality, 21 September 2013. See also https://en.wikipedia.org/wiki/Datagram_Congestion_Control_Protocol.

[26] The original design of the Internet architecture was based on "end-to-end connectivity" by virtue of which the end-points of the network are able to send and receive data-packets to and from other end-points, in a decentralised fashion. Therefore, the Internet was conceived as a "dumb" network, with "intelligent" edges that did not require operators to control or interfere in information's transmission. As World Wide Web inventor, Sir Tim Berners-Lee, has prominently argued, "[w]hen I invented the Web, I didn't have to ask anyone's permission. Now, hundreds of millions of people are using it freely. I am worried that that is going to end [...]. There have been suggestions that we don't need legislation because we haven't had it. These are nonsense, because in fact we have had net neutrality in the past -- it is only recently that real explicit threats have occurred". See: Tim Berners-Lee, *Net Neutrality: This is serious*, 2 June, 2006

[27] See: BEREC, *Overview of BEREC's approach to net neutrality*, op. cit.,

[28] See: Tim Wu, "Network Neutrality, Broadband Discrimination", in *Journal of Telecommunications and High Technology Law*, Vol. 2, p. 141, 2003.

[29] Like other "essentially contested concepts" such as freedom and democracy, openness is a powerful idea but requires to be further specified in order to be put in practice. Indeed, although different stakeholders may agree on the necessity to preserve freedom, democracy or openness, they may strongly disagree on how to implement such concepts by reason of their inner economic, social and political perceptions of such composite ideas and, consequently, the different degree of importance they attribute to specific facets of these concepts. See: Walter Bryce Gallie, "Essentially Contested Concepts", in *Proceedings of the Aristotelian Society*, New Series Vol.56, 1956, pp. 167-198.

II. Internet traffic management issues

"If you like it when some big multinational corporation controls what you see and where you see it and when you see it, then you shouldn't care. But if you like the fact that you control your Internet experience, and you want it to stay that way, then you should care."

Gigi Sohn - president of consumer advocacy group Public Knowledge

24. At present, certain ITM techniques allow ISPs to block, downgrade or prioritise specific data flows, thus providing ISPs with the ability to discriminate between online applications, services, content and devices. Such discrimination constitutes an interference with the neutral 'best-effort'[30] delivery model, typically exemplified by the 'first-in, first-out' ("FIFO")[31] routing technique, which is fully application-agnostic[32] and has been the standard on the Internet thus far.

25. It is important to note that ITM measures can be deployed for both legitimate and illegitimate purposes. A purpose which is clearly legitimate, for example, is to preserve the integrity and security of the network. To this latter extent, ISPs' capability to block certain traffic relating to malware and (D)DoS-attacks clearly serves the legitimate interests of the end-users of the network. On the other hand, a purpose which is undeniably illegitimate is to reduce the competition which online services pose to other services offered by ISPs (or their partners). An example of this is the blocking of Voice over Internet Protocol (VoIP) services, such as Skype, in order to reduce competition to traditional telephony services offered by ISPs or to those content and application providers ("CAPs") with which they vertically integrate.

26. It should be noted that, according to traditional economic reasoning, in an ideal situation, competition-law principles and commitment to transparency would be sufficient to grant both an efficient market and an efficient allocation of speech, allowing end-users to "vote with their feet" by abandoning network operators that unduly discriminate amongst applications, content, services and/or devices and do not respect Internet users' fundamental rights. However, a "market-based" approach to free speech has the fundamental flaw that an economically 'efficient' distribution of speech may not necessarily guarantee the full enjoyment of freedom of expression by every

---

[30] The concept of "best effort delivery" "refers to the way in which data is conveyed over the Internet – namely operators transmitting data streams to convey them from their point of departure to their destination, with no guarantee on performance but only an obligation of best endeavor". See: ARCEP, Report to Parliament and the Government on Net Neutrality, September 2012, p. 16.

[31] The expression FIFO with respect to Internet routing stems from Jerome H. Saltzer, David P. Reed & David D. Clark, "End-to-end arguments in system design", in *ACM Transactions on Computer Systems* n°2, 1984.

[32] The concept of application-agnosticism will be analyses in paragraphs 79 - 82.

individual. Indeed, if information flows were to be determined primarily or even solely by profit maximisation criteria, there could be a serious risk that commercial speech would crowd out all other forms of speech.[33]

27. Also, it should be noted that markets for Internet-access are commonly characterised as oligopolistic and particularly complex[34]. Notably, the inherent complexity of Internet-service markets is illustrated by non-intelligible consumer information, "product differentiation in the market for Internet access and for wireline and wireless bundles, and switching costs" which confine "the effectiveness of competition and reduce consumers' willingness to switch".[35] Such findings explain why market incentives and currently existing regulation based purely on economic and competition-law principles have thus far failed to fully enforce the network neutrality principle, to the detriment of the openness and 'public service value'[36] of the Internet.

28. Indeed, research by the Body of European Regulators of Electronic Communications ("BEREC") has shown that several types of restrictions are frequently implemented by European ISPs. For instance, BEREC has found that at least 20% of all European Internet users and potentially up to half of all mobile Internet-users undertake contracts that allow restriction of specific applications or services such as VoIP or P2P. Notably, about 90% of operators defining contractual restrictions on P2P enforce them technically, whilst contractual restrictions pertaining to VoIP are technically enforced by more than half (56%) of the mobile operators. In addition, it should be highlighted that end-users are

---

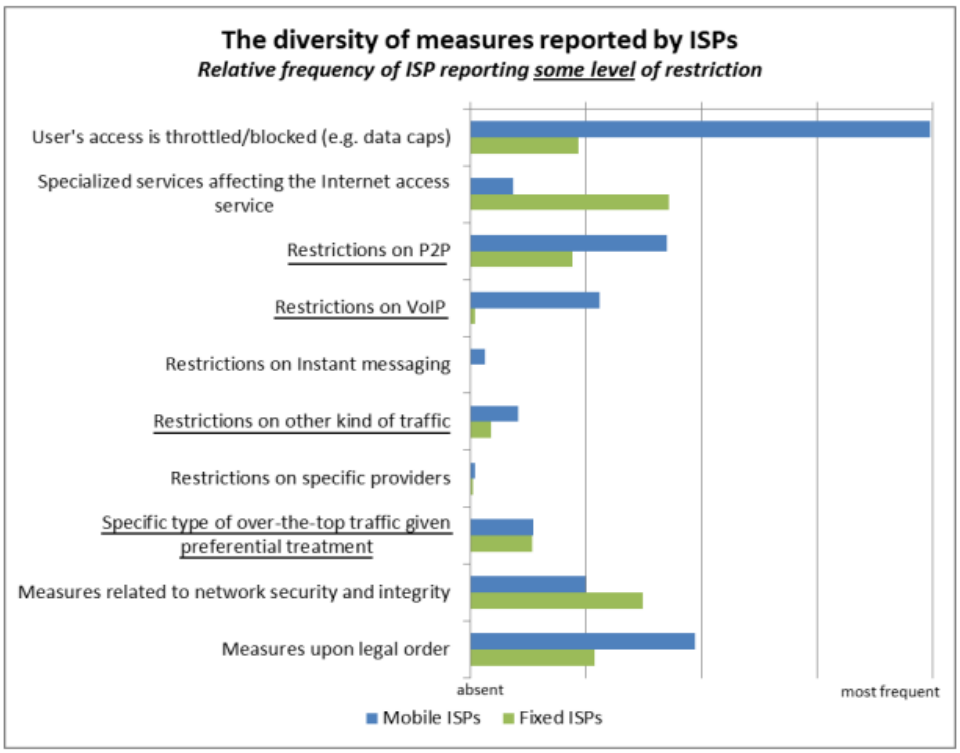
[33] To this extent, Jack Balkin argues that "[r]ecognizing that there is money to be made in advertising, sales, and delivery of content, telecommunications companies do not want to be pure conduits for the speech of others, and they do not want too much content competition from their customers. Instead, they want to use the architecture of the Internet to nudge their customers into planned communities of consumerist experience, to shelter end users into a world that combines everyday activities of communication seamlessly with consumption and entertainment. In some respects, businesses seek to push consumers back into their pre-Internet roles as relatively passive recipients of mass media content. In other respects, however, they openly encourage interactivity, but interactivity on their terms—the sort of interactivity that facilitates or encourages the purchase of goods and services." See: Balkin J., "Digital Speech and Democratic culture: a Theory of Freedom of Expression for the Information Society", in New York University Law Review, Vol 79:1.

[34] To this extent see e.g.: Faratin P. *et al.,* "The Growing Complexity of Internet Interconnection", in *Communications & Strategies* n° 72, 4th quarter 2008; Zhu K., "Bringing Neutrality to Network Neutrality", in *Berkeley Technology Law Journal*, vol. 22, n° 615, 2007.

[35] See: Van Schewick B., *Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like*, June 11, 2012, p. 37. Key economic barriers to enter into ISP markets include the need for digging trenches, laying pipes and wires and installing wireless transmission towers. As a consequence, typically there are only a few market players who are effectively in control of the transmission of Internet traffic to end-users in a particular geographic market. See: http://www.econtalk.org/archives/2010/04/benkler_on_net.html. Furthermore, it is deemed likely that if ISPs differentiate their Internet access services based on discriminating between content, applications, services and devices, the level of competition between ISPs would deteriorate. More content-level discrimination would make Internet access services less homogenous and less interchangeable. Consequently, competition on what should arguably be the most relevant competition-factors in Internet access service, bandwidth and price, is weakened by content-discrimination. See: Statistics Netherlands, Reaction of Statistics Netherlands to the internet consultation of the European Commission.

[36] See: Council of Europe, *Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet*.

usually unaware of the deployment of the aforementioned restrictions by their ISPs. Such an information-deficit holds promise to harm Internet users in their capacity to be well-informed consumers and may drive them to blame a supposed inefficiency of specific applications or services, not having the technical means and knowledge necessary to detect the existence of the aforementioned ITM measures. [37]



Source: BEREC, A view of traffic management and other practices resulting in restrictions to the open Internet in Europe.

29. As a further example, it may be recalled that in January 2012, four different British operators filtered the TOR-project website[38] (a website offering privacy-enhancing technologies), whilst, in February 2012, access to the website of La Quadrature du Net (an advocacy group) has been blocked by another mobile operator.[39] It seems obvious that the deployment of ITM measures to arbitrarily censor "inconvenient" opinions, or to make anonimising tools inaccessible, pose a serious threat to freedom of expression online[40]. After all, freedom of expression is 'rooted in anonymity'[41], and when

---

37 In this context, it should be noted that Alejandro Pisanty has suggested a risk management framework aimed at identifying and weighing network neutrality violations according to their likelihood and impact. In addition Pisanty's framework proposes actions for risk avoidance, detection, mitigation, business continuity, contingency planning, and prevention. See: Pisanty A. "Network Neutrality under the Lens of Risk Management", in Belli L. & De Filippi P. (ed.*), The Value of Network Neutrality for the Internet of Tomorrow, op. cit*, .pp. 61-70.

38 See: "A tale of new censors - Vodafone UK, T-Mobile UK, O2 UK, and T-Mobile USA", January 17th, 2012.

39 See: Orange UK blocking La Quadrature du Net, February 15, 2012.

40 For a country-specific analysis of technical filtering in the context of Internet censorship, see: OpenNet Initiative, *Country Profiles*, available at https://opennet.net/country-profiles.

advocacy groups are restricted in their ability to impart ideas, it can be argued that democracy itself has effectively been sabotaged.

30. In addition, it is important to highlight that, even if ISPs have transparent ITM policies as the current EU regulatory framework strives to achieve, ISPs are not automatically subject to the same due-process and human rights requirements that govern the activity of public entities in Europe. It should be remembered that ITM measures, such as filtering, may be imposed by national legislation in order to tackle a specific pressing social need,[42] but states can only impose such measures when a strict legal framework is in place, regulating the scope of the measures and affording the guarantee of judicial review to prevent possible abuses.[43] Indeed, being a restriction to the right to freely impart and receive information, the use of ITM techniques for law-enforcement purposes is required to be in accordance with the rule-of-law and due-process principles prescribed by Article 10, paragraph 2 of the ECHR.

31. Since most people can acquire access to the Internet only from private ISPs rather than from publicly owned ones, and given the important public service value of the Internet in providing an open platform for people to engage in social, economic and political activities within the information society, there is a strong case to be made for the imposition of similar due process and rule of law requirements to private ISPs, as those which apply to public bodies.[44] In this respect it must be underlined that the Internet is used for much more than just commercial purposes. This latter element may provide an important indication that allowing commercial entities – which are by definition primarily concerned with maximising economic profit – full, unchecked control over Internet traffic flows, could pose a serious threat to the multitude of non-commercial uses permitted and fostered by the Internet, having the potential to diminish the freedom and autonomy of individuals within the information society, particularly those who are less wealthy.

32. Furthermore, as highlighted on several occasions by the European Data Protection Supervisor, the utilisation of certain intrusive ITM techniques – such as Deep Packet Inspection ("DPI") – has

---

41 La Rue F., Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011, nr. A/HRC/17/27.

42 For example, in multiple countries ISPs have been ordered by courts to filter the file-sharing website thepiratebay.org (and a number of mirrors and proxies).

43 See: Ahmet Yıldırım v. Turkey (Application n° 3111/10) [2012].

44 Meaning: no discrimination, restriction or interference, unless strictly necessary for and proportionate to a narrowly circumscribed legitimate aim. Such requirements may also imply safeguards against being disconnected from the Internet. Arguably, ISPs should only be allowed to disconnect their subscribers and terminate their agreements, if the subscriber is (sufficiently far) behind on payments and not based on which use the subscriber has made of the Internet access services.

serious implications in terms of privacy of communications and data protection.[45] Indeed, DPI allows a particularly granular analysis of each data-packet being sent over a specific network and may be used by ISPs to inspect the content of end-users' communications and consequently distinguish the treatment of each type of packet according to predefined criteria.[46] DPI allows to scrutinise the "payload" (*i.e.* the content) of each data-packet, in addition to the "header" that is the 'exterior' part containing the metadata that direct packets to their destination. Using the traditional postal services as a metaphor, the payload may be equated to the content of a letter (*i.e*. images, text, handwriting style, *etc*.) whilst the header could be seen as the address that directs the letter to the recipient.

33. Although the utilisation of DPI may be particularly lucrative for ISPs, allowing them to combine technological efficiency with the maximisation of their economic profits,[47] it should be stressed that this technique holds promise to interfere with end-users fundamental right to privacy as well as with their freedom of expression. Continuing with the postal analogy: would it be acceptable if the mailman opened every letter, and would then, based on the contents and the identity of the sender and receiver, decide (i) how much delivery would cost, (ii) which letters would be delivered first and (iii) which letters would not be delivered at all? In this context it should also be noted that it appears technically possible to use DPI to modify[48] the contents of packets and identify data traffic even when it is encrypted.[49] Indeed, due to their natural gatekeeping position, ISPs are ideally situated to monitor, mine, and modify data using the DPI appliances within their network.[50]

34. The fact that DPI is being put in place by private actors also raises concerns with regard to due-process and rule-of-law requirements. As it cannot be assumed that market incentives alone will

---

[45] See: European Data Protection Supervisor, *Opinion on net neutrality, traffic management and the protection of privacy and personal data*, 7 October 2011, p. 8.

[46] Originally, DPI was conceived to secure local area networks (LANs) thus filtering out unsolicited communications coming in from other networks. In addition to network security, DPI is also used for bandwidth management, advertisement targeting, copyright-content filtering and government surveillance. See: Bendrath R., *Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection*, March 2009

[47] To this extent Lessig and McChesney argued that filtering capabilities such as DPI can allow ISPs to differentiate data flows, "sell[ing] access to the express lane to deep-pocketed corporations and relegate[ing] everyone else to the digital equivalent of the winding dirt road". See: Lessig L. & McChesney R.W., *No Tolls on the Internet Washington Post*, 8 June 2006.

[48] To this extent, it should be noted that "[m]odification and Injection applications examine content and modify packet content for a variety of purposes, such as to insert tracking ids, rewrite packet headers […], and may inject new packets or traffic as a result (for example: injecting TCP resets to interfere with P2P traffic). See: Radisys, *DPI: Deep Packet Inspection Motivations, Technology, and Approaches for Improving Broadband Service Provider ROI*, September 2010, p.4

[49] See: Daly A., "The legality of deep packet inspection", in International Journal of Communications Law and Policy, 2011

[50] See: Parsons C., *Literature Review of Deep Packet Inspection: Prepared for the New Transparency Project's CyberSurveillance Workshop*, version 4.1, 6 March 2011.

provide sufficient protection of the users' privacy interests,[51] these intrusive techniques should be scrutinised by the national data-protection authorities and their use should be allowed only if necessary and proportionate to the achievement of narrowly circumscribed legitimate purposes and in accordance with national legislation.[52]

35. Lastly, it should be noted that it is currently hotly contended whether it is legitimate to prioritise traffic on certain still to be created interconnected IP-based networks, which may not be strictly considered as part of the Internet but which apparently would share capacity with the Internet, over Internet traffic, in order to achieve a guaranteed quality of service ("QoS") – or an assured service quality ("ASQ")[53] – particularly when the intended business model is to charge additional fees and use alternative payment models, such as Sending Party Network Pays ("SPNP"),[54] for this prioritised service.

36. On the one hand, the proponents of this model, such as the European Telecommunications Network Operators' Association ("ETNO") and Economics and Technologies for Inter-Carrier Services ("ETICS") consortium, argue that prioritised delivery to achieve QoS or ASQ is necessary to guarantee the proper functioning of certain applications with more stringent transmission requirements, such as a low tolerance to jitter and delay. Examples of such applications include video-streaming, VoIP, online gaming and e-health applications. [55]

37. On the other hand, various civil society groups and scholars fear that such initiatives could herald the demise of the open Internet and should not be adopted. ETNO's proposals to the ITU World Conference on International Telecommunications (WCIT) for example,[56] were strongly criticised, most notably by BEREC, who argued that this proposal was "advocating an 'interconnection

---

51 It should be noted that existing European telecom regulations currently already contain many provisions on privacy, imposing obligations on service providers to respect and actively protect user privacy.

52 To this extent, Chris Marsden highlights that "[i]ncreasing use of DPI is being created for both Western ISPs and more autocratic governments. In both cases, the method chosen is co-regulation –the government sets the rules and the ISPs are allowed a broad measure of independence as to process to achieve the results the government sets out. This is controversial in that it passes powers to control freedom of expression into private hands, often without the constitutional protections that govern public authority intervention and censorship". See: Marsden C.T., *Net Neutrality Towards a Co-regulatory Solution*, Bloomsbury Academic, 2010, p. 19.

53 See e.g. ETICS Deliverable D4.3: 'Revision of ETICS Architecture and Functional Entities'.

54 See e.g. ETICS Deliverable D3.5, 'Final Business Models Analysis'.

55 I.e. applications that are 'real time' or interactive and use a lot of bandwidth. It is important to note that the applications which are mentioned as examples by ETICS and ETNO, currently already exist on the public Internet.

56 In 2012 ETNO argued for the ITU to include an explicit reference in the International Telecommunications Regulations (ITRs) to SPNP and to the concept of end-to-end QoS delivery on interconnected networks, in order to create alternative Interconnected IP networks next to the Internet, where the basis for commercial negotiation would "not be the volume of the traffic exchanged between parties, or the "bit rate at the interconnection points" but the "value" that the traffic represents for the ecosystem." See: ETNO paper on Contribution to WCIT ITRs Proposal to Address New Internet Ecosystem.

philosophy' based on transmission services being provided across the Internet all along a defined path between endpoints, much like the connection-oriented circuit switched 'old generation' PSTN networks and voice services on which ETNO members built their businesses." According to BEREC, "This is fundamentally at odds with the principles of connection-less packet switched networks underlying the success of the Internet to date, based on decentralisation and simplicity", and such models could undermine the continued development of the open, dynamic and global platform that the Internet provides, and therefore lead to an overall loss of welfare.[57]

38. Although the aforementioned proposal was not successful, in June 2013 a three year research project by ETICS was completed[58] which provides business models and technical models to implement ASQ on multiple, interconnected IP networks.[59]

39. Opponents of such models claim that prioritizing traffic flows on multiple interconnected IP-based networks has many more significant drawbacks than advantages, particularly when many networks are interconnected, like on the Internet.[60] To this latter extent BEREC has explicitly highlighted that "Over the Internet, a guaranteed end-to-end QoS offer is […] neither commercially nor technically realistic."[61]

40. In line with other reasons noted by BEREC, this can be attributed to the fact that the ability to *guarantee* a speedy and timely delivery of traffic through prioritisation is claimed to be limited, because when the network is truly very congested, even packets with a higher priority will still not arrive in time, whereas at times of very little or no congestion, higher priority does little or nothing to improve delivery over lower priority.

---

[57] BEREC, BEREC's comments on the ETNO proposal for ITU/WCIT or similar initiatives along these lines, BoR (12) 120 rev.1, 14 November 2012.

[58] The ETICS project is stated to have cost 12.8 million euro, 8 of which was sponsored by the EU: see https://www.ict-etics.eu/overview/project-facts.html.

[59] Similar to ETNO's ITU proposal, ETICS' business models document appears to argue that the business model for the current neutral Internet is, for various reasons and in various situations, not sustainable and would better be supplemented, or possibly even replaced, by alternative payment models, such as SPNP. See ETICS Deliverable D3.5, 'Final Business Models Analysis'. "At the same time, the traditional peering and transit interconnection agreements do not provide any type of QoS assurance. Those agreements are service-agnostic and pertain to interdomain traffic aggregates of multiple services (elastic and inelastic), which all experience an unpredictable network QoS that mostly depends on overprovisioning mechanisms, which are both insufficient and inefficient [ATKearney10], [Jacobson09], [OECD12], [Walrand08]. Paired with the increasing overall traffic demand (and the associated investment requirements) and the limited incentives in investing in new core and interconnection technologies, this inevitably renders the current technological and business landscape unsustainable for the provisioning of the emerging services that rely on predictable network performance.

[60] For instance, see: Huston G. APNIC, RIPE 65, September 2012, 'The Concept of Quality of Service in the Internet'.

[61] BEREC also notes that "While mechanisms for introducing differentiated QoS traffic classes have been available for more than a decade, […] these have not been implemented across networks on the Internet (as opposed to the provision of specialised services within operators' own networks, e.g. in relation to IPTV)." On the other hand, it is also appropriate to note that market regulators may not always be right in predicting how development of technology plays out and that legislators and regulators should therefore be cautious and limit only those specific technological developments which would undermine important policy objectives, but allow all other developments.

41. This also explains why many observers expect that 'pay-for-priority' business models actually reduce incentive in expanding network capacity rather than encourage investment.[62] Indeed, in order to be able to profit from prioritisation, a certain level of congestion is a prerequisite. Therefore, even if a rule is adopted which disallows outright blocking and throttling of traffic for illegitimate reasons, there seems to be a risk that expansion of capacity on the Internet would be slowed down, should guaranteed QoS or ASQ interconnection gain popular adoption. Furthermore, if such products would share capacity with the public Internet and get priority over it, one could argue that this in fact entails a form of throttling the public Internet.

42. Another important obstacle to achieve guaranteed QoS or ASQ on interconnected IP-based networks, or even the Internet itself, is the necessity that all networks reach agreement on what traffic must be prioritised and when. Importantly, if the goal is to *sell* priority on the interconnected IP-based network to content and application providers, this would require commercial agreements on priority (and probably pricing) spanning across all (competing) networks. Creating such necessary agreements can be expected to be complex and costly, and, moreover, it appears that this process may risk triggering the creation of a large cartel and severely diminish competition[63].

43. As was argued in part I, the predominantly neutral, best-effort transmission of Internet traffic is a major contributing factor in achieving the desired openness of the Internet. Resorting to centralised interference and discrimination in the network in order to give a better transmission quality to certain applications while downgrading others, has the potential to limit the openness of the Internet, inflate barriers and restrict the free flow of information, thus negatively affecting pluralism[64] as well as the full, free and equal enjoyment of human rights. Therefore, such interferences should be minimised as much as possible, whilst the least discriminatory means possible should be employed to enable applications with specific QoS-requirements, in accordance with the criteria of proportionality and subsidiarity.

44. Such reasoning implies that the expansion of bandwidth and capacity is normally the best solution to promote and enable innovative applications, thus facilitating a "virtuous cycle"[65], whereas discriminatory treatment cannot be justified unless it occurs in a time-limited fashion, *e.g.* in order to mitigate the effects of exceptional and temporary congestion. If it is claimed that the expansion of

---

62 See: BEREC, Differentiation practices and related competition issues in the scope of Net Neutrality, May 2012, p. 4.

63 See e.g. La Quadrature du Net, *Neelie Kroes Pushing Telcos' Agenda to End Net Neutrality,* 30 August 2013.

64 To this end, see: High Level Group on Media Freedom and Pluralism, *A free and pluralistic media to sustain European democracy*, January 2013.

65 FCC 10-201, report and order on the open Internet 2010, paragraph 14.

capacity is not viable in certain situations, making discriminatory solutions necessary,[66] such claims must be critically examined and if necessary, alternative funding models for the expansion of capacity should be considered.[67]

45. Duly recognising the limitations of automotive analogies to portray IT-related policy issues on a detailed level, it may be helpful to illustrate this situation by comparing digital highways with physical ones. To this end, it may be argued that as a general rule, in order to achieve better mobility and stimulate a free flow of traffic, it should be considered wiser, more efficient and more fair to invest in building more and wider roads for all, rather than giving motorists the ability to pay for green lights, or allow private companies exploiting roads to make deals that would make traffic lights continuously green for expensive supercars, but red for economy cars.

46. Therefore, the fact that Internet access, which is nowadays essential for the participation in democratic life[68], is provided by commercial entities, poses particular risk. As commercial actors which only, or at least primarily, pursue the maximisation of their profits, ISPs may not be concerned about the provision of unfiltered and diverse information, which is the basis of the public service value of the Internet.[69] If it is possible to expand profits by monetising discrimination as the epicentre of a two-sided market, in lieu of making investments to expand capacity for all, it begs the question if a commercial entity – on its own volition – would choose the option that is more expensive and may yield less short term profit, even if that option would provide the most public benefit.

47. If it were the case that commercial entities in a free (but nonetheless already quite heavily regulated) market do not wish to invest in creating (over)capacity to provide for non-discriminatory delivery of Internet traffic, rather preferring to try to monetise network congestion, it could be worth considering, besides enacting rules which outlaw selling of priority, to organise the expansion of the

---

66 ETICS, Final Business Models Analysis, Deliverable: D3.5, version 1.0, 15 January 2013.

67 In this respect it is not difficult to understand why civil society organizations like La Quadrature du Net appear to be slightly outraged by the fact that 8 million euros of EU taxpayers' money was spent on research relating to discriminatory 'future networks', and therefore was not spent on new fibre infrastructure in order to expand capacity of the open and neutral Internet for everybody. See e.g. La Quadrature du Net, *Neelie Kroes Pushing Telcos' Agenda to End Net Neutrality, op. cit*.

68 See, e.g.: French Constitutional Council, Decision No. 2009-580DC of the 10th of June 2009; La Rue F., 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *op. cit.*

69 It is important to underscore that open electronic networks based on the Internet Protocol have an important public function, being one of the principal means of exercising the right to freedom of expression and information, and playing an essential role in letting individuals participate freely, fully and safely in democratic life . To this extent, the Council of Europe has highlighted the public service value of the Internet – which is grounded on the consideration that every individual has the right to fully benefit from the information society, receiving trustworthy and diverse information – and has recommended to the Member States to elaborate a clear legal framework delineating the boundaries of the roles and responsibilities of all key stakeholders in order to impede that the use of ICT could adversely affect any fundamental rights. See: Council of Europe, *Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet*.

digital infrastructure by means of public contracts, just as with physical roads, and then hold tenders to grant right to provide non-discriminatory Internet access and transit services on this infrastructure to the best suited entity. Such an option could indeed allow the maximisation of the public service value of the Internet and safeguard its openness. The fact that this model is already utilised in various forms across municipalities and regions in different member states of the Council of Europe and on other continents,[70] may serve as a testament to its viability, while it would likely be beneficial to also conduct further studies to analyse the indications and contra-indications for the implementation of such models in various specific circumstances (e.g. density of population, wealth and existing infrastructure capabilities). In addition, should be underlined that any broadband infrastructure model which ascribes a crucial role to the state must be accompanied by clear and stringent due-process and human rights requirements.[71]

48. Furthermore, the idea of 'homes with tails' as an alternative funding model for the creation of next generation digital (fibre) infrastructure could also serve as an example how non-discriminatory future networks may be realised instead of discriminatory ones.[72] It must be reminded that it follows from the principle of subsidiarity that the least discriminatory means to achieve a legitimate aim, in this case the expansion of digital broadband infrastructure, should be utilised.

49. Another option still, has been suggested by net neutrality scholar Christopher Marsden. According to Marsden it may be necessary to legally require that specialised services – *i.e.* those services provided and operated within closed IP based networks, "often optimised for specific applications based on extensive use of traffic management in order to ensure adequate service characteristics"[73] – be accompanied by an investment plan to increase public Internet capacity as well. In order to enforce this requirement, the relevant NRA could be tasked to perform audits on an annual basis to ensure that the capacity is actually deployed and that public Internet capacity continues to grow per subscriber. [74] However, given the fact that there are other options available for the expansion of the capacity of the open Internet as well, and since it is by no means a certainty that

---

70 See: Berkman Center for Internet & Society at Harvard University, *Next Generation Connectivity: A review of broadband Internet transitions and policy from around the world*, February 2010.

71 When broadband infrastructure is owned by a public entity, that entity is in a position to impose certain requirements to the commercial ISPs delivering Internet access services on that infrastructure. It should be ensured that such requirements are in the sphere of safeguarding openness, universal access and network neutrality, rather than government-mandated interferences.

72 See: Slater D. & Wu T., *Homes with Tails: What if You Could Own Your Internet Connection?*, in New America Foundation Wireless Future Program, Working Paper #23. 2008.

73 See: BEREC, *BEREC Guidelines for quality of service in the scope of net neutrality*, BoR (12) 131, 26 November 2012, p. 4.

74 See: Marsden C.T., *Question for IGF net neutrality coalition: Regarding specialised service*, 18 September, 2013.

ISPs would not be willing to invest in expanding such capacity on their own volition, the legal requirement to invest in network capacity and its supervision by NRAs may at this stage be deemed as a regulatory excess. In this context, it should also be noted that tax benefits may also be employed to provide a positive 'nudge' as an incentive to invest, instead of a forceful regulation.

50. In any case, nothing should preclude that network providers and network users agree on a defined quality of service or assured service quality, as long as such agreement does not imply the imposition of discriminatory treatment of Internet traffic, where the highest bidder gets to have priority over all the others, or where specific Internet traffic is throttled or blocked.

51. To conclude, it is essential to remind that, although private entities – such as ISPs – are not directly subject to ECHR provisions, "[n]othing in [the ECHR] may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention."[75] Hence, the application of obligations to respect network neutrality on ISPs is perfectly compatible with the ECHR and may be particularly helpful to elucidate the modality according to which fundamental rights should be implemented in the electronic communications context[76].

52. Moreover, in order to safeguard the public service value of the Internet, "Member states should adopt or develop policies to preserve and, whenever possible, enhance the protection of human rights and respect for the rule of law in the information society"[77], paying particular attention to the need to ensure that there are no restrictions to fundamental human rights other than to the extent permitted by the ECHR, as interpreted by the ECtHR. Hence, in light of the aforementioned concerns raised by ITM measures, the strong enforcement of the net neutrality principle must be considered as a priority for member states of the Council of Europe, in order to safeguard the full enjoyment of end-users' fundamental rights granted by the ECHR.

---

[75] See: article 17 ECHR. To provide further explanation why the free speech interest of Internet users to communicate freely without interference should prevail over a free speech interest of ISPs to not transmit certain information, we may again refer to a postal analogy. A notion of the postal service basing a claim on its freedom of speech to not deliver letters which it does not like the contents of, can be considered as quite absurd.

[76] This purpose is particularly evident at the EU level where, paradoxically, the Framework Directive states that "[m]easures taken by Member States regarding endusers access' to, or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law", whilst BEREC explicitly claims that "intervention in respect of [fundamental rights] considerations lies outside the competence of [NRAs]." See: Directive 2002/21/EC, article 1.3a, as amended by directive 2009/140/EC; *BEREC Response to the European Commission's consultation on the open Internet and net neutrality in Europe*, 30 September 2010, BoR (10) 42

[77] See: Council of Europe, Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, op; cit.

53. The need for a specific legal framework protecting network neutrality is therefore threefold. In addition to (i) allowing Internet-users to fully enjoy their fundamental rights, net neutrality protection is fundamental (ii) to guarantee that the Internet maintains its public-service value, as it has been stressed by the Council of Europe Committee of Ministers since 2007, and reinvigorates the end-to-end principle, thus (iii) encouraging Internet users' proactive role in the dissemination of innovation.

III. A model framework and its application

"Yes, regulation to keep the Internet open is regulation. And mostly, the Internet thrives on lack of regulation. But some basic values have to be preserved."

Sir Tim Berners-Lee, World Wide Web inventor

54. According to the Internet Governance Strategy 2012-2015, the Council of Europe shall develop "human rights policy principles on 'network neutrality' to ensure Internet users have the greatest possible access to content, application and services of their choice as part of the public service value of the Internet and in full respect of fundamental rights".[78] Indeed, in order to effectively enable the protection of a fundamental right, it is often necessary to enact specific legislation to that effect.[79] To this end, it is important that the member states of the Council of Europe recognise a positive obligation to protect net neutrality in order to guarantee European citizens' ability to freely use the Internet to participate in democratic, economic and social life.[80] Furthermore, because the network neutrality principle is also instrumental to ensure pluralism in the information society, it can be argued that Council of Europe members' positive obligation to guarantee effective media pluralism[81] also implies a positive obligation to protect net neutrality.

Notably, the enforcement of the network neutrality principle should be put in place through:

a) A clear legal framework aimed at safeguarding the public service value of the Internet and upholding citizens' human rights and fundamental freedoms;

---

78 See: Council of Europe, *Internet Governance, Council of Europe Strategy 2012-2015*, paragraph I.8.e, op. cit.

79 In this regard it can be noted that many members of the Council of Europe have already enacted specific data protection legislation to protect and effectively enable the fundamental right of its citizens to privacy, and have already enacted specific non-discrimination legislation to effectively protect citizens against illegal discrimination based on race, gender, sexual preferences and other properties.

80 See: Marsden C.T., University of Sussex, *(Pre)-history of European Network Neutrality and Human Rights*, Strasbourg, 29 May 2013.

81 Centro Europa 7 S.r.l. and Di Stefano v. Italy (application no. 38433/09)([2012] ECHR 974).

b) the clear definition of legitimate purposes for ITM measures, and the establishment of predefined criteria to evaluate whether they are justified. The delineation of such criteria seems indeed essential to grant universal and reciprocal access to all resources connected to the Internet and to guarantee that interference with end-users' fundamental rights only occur when necessary for and proportionate to their legitimate aim;

c) the clear definition of the role and responsibilities ascribed to the public authority which must enforce the network neutrality principle, having particular regard to its human rights dimensions.

55. It is important to acknowledge that by granting universal and reciprocal access to online resources, the network neutrality principle stimulates not only freedom of expression, but also innovation and investments in both online applications, services, content and devices, as well as the expansion of network capacity.[82] Indeed, online content, applications, services and devices are the true *raison d'être* of the Internet, because "[w]ithout email, the Web, instant messaging, VoIP and so on, the Internet would be (literally) useless"[83]. To this extent, a recent study has shown that the enshrinement of network neutrality into regulation "increases particularly the incentives of small innovators" and this innovation-galvanisation effect determines "positive network externalities [that] can be internalized at the benefit of end users and innovators".[84]

56. For this reason, it does not seem justified to argue that network neutrality reduces ISPs' revenues, because it rather appears to result in increasing end-users' demand, while still allowing ISPs to differentiate their offer in a non-discriminatory fashion (*e.g.* by offering higher bandwidth for higher prices). Hence, network neutrality and openness should be deemed as true catalysts for innovation, for they provide a number of opportunities to increase ISPs' revenues and, consequently, to encourage investments.[85]

57. Furthermore, although traffic prioritisation might be particularly lucrative for ISPs,[86] it seems fallacious to argue that traffic discrimination is actually necessary to cope with the increase of data

---

[82] To this extent, see e.g.: Felten B, There's No Economic Imperative to Reconsider an Open Internet, April 3, 2013; Williamson B., Black D. & Punton T., The open internet – a platform for growth, October 2011.

[83] See: Clark D.D. & Blumenthal M.S., "The end-to-end argument and application design: the role of trust", in *Federal Communications Law Journal*, vol. 63, n°357, 2011.

[84] See: Kocsis V. and Weda J*, The innovation-enhancing effects of network neutrality,* study commissioned by the Dutch Ministry of Economic Affairs, Amsterdam, 12 June 2013, p. 19.

[85] See: Frode Sørensen, *10 myths about net neutrality*, March 2013.

[86] In February 2010, for instance, president of Spanish telecoms operator Telefónica, César Alierta, stated that "Internet search engines use our net without paying anything at all, which is good for them but bad for [Telefónica]. It's obvious that this situation must change. Our strategy is to change this". See: Latif L., *Telecom operators are starting to jump off the fence*, 20 September, 2010.

volumes. Indeed, it should be stressed that, in spite of the current increase of Internet traffic volume per user, unit costs for network equipment are declining at an equal rate[87] while "Western European fixed Internet traffic is growing at only 17% CAGR and mobile at 50% or lower […]. Both are historically low figures, suggesting the opposite of a 'data explosion'".[88] Consequently, it seems that "costs, prices, and the number of subscribers are growing in balance with one another overall". [89]

58. Moreover, it should be noted that CAPs like Facebook or YouTube, are already required to remunerate ISPs in order to be connected to the Internet. The fees that CAPs have to honour are generally commensurate with the volume of bandwidth they require, or can be defined through peering agreements[90].

59. To this extent, it should be noted that business agreements establishing prioritised traffic delivery within the public, best-effort Internet would diminish ISPs' incentives to invest in network enhancement, by permitting them to benefit from the scarcity of their network's bandwidth. Indeed, should prioritisation be commercially traded, it seems obvious that the existence of network congestion would become a source of profits, because the existence of congestion would actually be required to trigger demand for prioritisation. Therefore, it must be acknowledged that the commercialisation of prioritisation is likely to determine strong incentives not to invest (too much) in infrastructure enhancement.

60. It is therefore essential to highlight that ITM measures consisting in prioritisation of "first-class" content, applications and services – i.e. no latency only for those who can afford the prioritisation fees – risk to undermine the public service value of the Internet while diminishing end-users' ability to enjoy a neutral, open and pluralistic Internet ecosystem. Indeed, it seems obvious that commercial agreements allowing specific CAPs to enjoy "first-class" delivery are likely to (i) determine the degradation of the "economy-class" contents, applications and services excluded by the agreements[91]; and to (ii) dangerously agglomerate power in the hands of ISPs, leading to private control over information flows and, subsequently, triggering a high risk of manipulation of public

---

87 See: Cisco, *Cisco Visual Networking Index: Forecast and Methodology, 2012–2017*, May 29, 2013 ; WIK-Consult, *op. cit.* p. 10.

88 See: Christopher T. Marsden, "Net Neutrality: Past Policy, Present Proposals, Future Regulation?" in Belli L. & De Filippi P. (ed.), The Value of Network Neutrality for the Internet of Tomorrow, *op. cit*., p.88.

89 As it has been argued by WIK-Consult, "costs are by no means exploding, and the costs that are alleged to be increasing would in any case be small compared to the overall costs of the business". See: WIK-Consult, *Network operators and content providers: Who bears the cost?*, 9 September 2011, p. 75

90 See: Kearney A.T., *A Viable Future Model for the Internet*, 2011, p. 7.

91 To this extent, see: eg Chirico F., Van der Haar I. and Larouche P., "Network Neutrality in the EU", TILEC Discussion Paper, 2007

opinion, or at least a disproportionate representation of commercial information over non-commercial information.[92]

61. In addition, it seems inappropriate to argue that the "best-effort" model, according to which Internet traffic is traditionally routed, implies a low level of network performance and is less economically efficient than traffic prioritisation. Indeed, the best-effort paradigm does not equate to low quality but merely suggests that best-efforts are applied indiscriminately to properly transmit all Internet traffic, while the same optimal level of performance (in terms of latency, packet loss, etc.) cannot be guaranteed permanently to any specific application.[93]

62. Therefore, it should be noted that, by impeding those interferences, restrictions and discriminations that are not under the direct control of the user, the network neutrality principle facilitates a virtuous circle[94], reinvigorating end-users' freedom of expression and unleashing their capacity to share their own innovations. Indeed, non-discriminatory traffic management fosters end-users' fundamental right to freely impart and receive information and ideas that, in turn, encourage innovation of content, applications and services. Therefore, network neutrality contributes to stimulate end-users' demand for internet access, increasing the need for faster broadband, wider mobile data coverage and further take-up of broadband and smart devices.[95]

63. For the reasons provided above, a strong protection of the network neutrality principle should be expected to be beneficial in order to enhance European citizens' wellbeing both from an economic and a human rights perspective. To enable the Council of Europe member states to maximise Internet freedom for their citizens, we suggest the following 'Model Framework on Network Neutrality' (hereafter also the "Model Framework", or the "Model".[96]

---

92 As highlighted by the High Level Group on Media Freedom and Pluralism, "the degree of control and censorship of the […] media has been in direct correlation with the degree of totalitarianism in a country's form of governance". See: High Level Group on Media Freedom and Pluralism, *A free and pluralistic media to sustain European democracy*, *op. cit.* p. 10.

93 To this extent, see : Sørensen F., 10 myths about net neutrality, *op. cit.*

94 To this extent, see: BEREC, *Differentiation practices and related competition issues in the scope of Net Neutrality*, *op. cit.*; Robin S. Lee and Tim Wu, "Subsidizing Creativity Through Network Design: Zero Pricing and Net Neutrality", in *Journal of Economic Perspectives,* vol. 23 n°3, 2009, pp. 61-76; Williamson B., Black D. & Punton T., The open internet – a platform for growth *op. cit*.

95 See: Plum Consulting, *The open internet – a platform for growth*, October 2011.

96 The Model has been the result of a collaborative effort put in place by the Dynamic Coalition on Network Neutrality (DC NN), an expert-group created under the auspices of the United Nations Internet Governance Forum. The first preliminary draft of the model framework has been elaborated by merging the two models proposed by Luca Belli and Matthijs van Bergen as an input for the Multi-Stakeholder Dialogue on Network Neutrality and Human Rights, organised under the aegis of the Council of Europe. This draft has been circulated on the mailing-list of the DC NN as a Request for Comments, with the purpose of seeking for advice, critiques and suggestions of all interested stakeholders through an open, transparent and inclusive process . The first comment-period lasted 30 days (from 25 July 2013 to 25 August 2013). After having consolidated the comments and inputs expressed by the DC NN members over this first comment

A Model Framework on Network Neutrality

1) Network neutrality is the principle according to which Internet traffic shall be treated equally, without discrimination, restriction or interference regardless of its sender, recipient, type or content, so that Internet users' freedom of choice is not restricted by favouring or disfavouring the transmission of Internet traffic associated with particular content, services, applications, or devices.

2) In accordance with the network neutrality principle, Internet service providers shall refrain from discriminating, restricting, or otherwise interfering with the transmission of Internet traffic, unless such interference is strictly necessary and proportionate to:

a) give effect to a legislative provision or court order;

b) preserve the integrity and security of the network, services and the Internet users' terminal equipment;

c) prevent the transmission of unsolicited communications for direct marketing purposes to Internet users who have given their prior consent to such restrictive measures;

d) comply with an explicit request from the subscriber, provided that this request is given freely and is not incentivised by the Internet service provider or its commercial partners;

e) mitigate the effects of temporary and exceptional network congestion, primarily by means of application-agnostic measures or, when these measures do not prove efficient, by means of application-specific measures.

3) The network neutrality principle shall apply to all Internet access services and Internet transit services offered by ISPs, regardless of the underlying technology used to transmit signals.

4) The network neutrality principle need not apply to specialised services. Internet service providers should be allowed to offer specialised services in addition to Internet access service, provided that such offerings are not to the detriment of Internet access services, or their performance, affordability, or quality. Offerings to deliver specialised services should be provided on a non-discriminatory basis and their adoption by Internet users should be voluntary.

5) Subscribers of Internet access service have the right to receive and use a public and globally unique Internet address.

6) Any techniques to inspect or analyse Internet traffic shall be in accordance with privacy and data protection legislation. By default, such techniques should only examine header information. The use of any technique which inspects or analyses the content of communications should be reviewed by the relevant national data protection authority to assess compliance with the applicable privacy and data protection obligations.

---

period, a reviewed version of the model framework has been circulated on the DC NN mailing list by the authors of this report for a second comment-period, lasting one week (from 8 to 15 September 2013). A third informal comment-period, lasting roughy one week, has been established to allow final remarks and objections. See: Belli L. & Van Bergen M., *A Discourse-Principle Approach to Network Neutrality: A Model Framework and its Application*, in Belli L. & De Filippi P. (ed.), The Value of Network Neutrality for the Internet of Tomorrow, Report of the Dynamic Coalition on Network Neutrality, 2013 and www.networkneutrality.info.

7) Internet service providers shall provide intelligible and transparent information with regard to their traffic management practices and usage polices, notably with regard to the coexistence of Internet access service and specialised services. When network capacity is shared between Internet access services and specialised services, the criteria whereby network capacity is shared, shall be clearly stated.

8) The competent national regulatory authority shall:

a) be mandated to regularly monitor and report on Internet traffic management practices and usage polices, in order to ensure network neutrality, evaluate the potential impact of the aforementioned practices and policies on fundamental rights, and ensure the provision of a sufficient quality of service and the allocation of a satisfactory level of network capacity to the Internet. Reporting should be done in an open and transparent fashion and reports shall be made freely available to the public;

b) put in place appropriate, clear, open and efficient procedures aimed at addressing network neutrality complaints. To this end, all Internet users shall be entitled to make use of such complaint procedures in front of the relevant authority;

c) respond to the complaints within a reasonable time and be able to use necessary measures in order to sanction the breach of the network neutrality principle.

This authority must have the necessary resources to undertake the aforementioned duties in a timely and effective manner.

9) Definitions

a) The “Internet” is the publicly accessible electronic communications network of networks that use the Internet Protocol for communication with endpoints reachable, directly or through network address translation, via a globally unique Internet address.

b) The expression “Internet service provider” refers to any legal person that offers Internet access service to the public or Internet transit service to another ISP.

c) The expression “Internet access service” refers to a publicly available electronic communications service that provides connectivity to the Internet, and thereby provides the ability to the subscriber or Internet user to receive and impart data from and to the Internet, irrespective of the underlying technology used to transmit signals.

d) The expression “Internet transit service” refers to the electronic communications service that provides Internet connectivity between Internet service providers.

e) The expression “Internet traffic” refers to any flow of data packets transmitted through the Internet, regardless of the application or device that generated it.

f) The expression “specialised services” refers to electronic communications services that are provided and operated within closed electronic communications networks using the Internet Protocol, but not being part of the Internet. The expression “closed electronic communications networks” refers to networks that rely on strict admission control.

g) The expression “application-agnostic” refers to Internet traffic management practices, measures and techniques that do not depend on the characteristics of specific applications, content, services, devices and uses.

h) The expression “subscriber” refers to the natural or legal person who has entered into an agreement with an Internet service provider to receive Internet access service.

i) The expression “Internet user” refers to the natural or legal person who is using Internet access service, and in that capacity has the freedom to impart and receive information, and to use or offer applications and services through devices of their choice. The Internet user may be the subscriber, or any person to whom the subscriber has granted the right to use the Internet

access service s/he receives. Any legal person offering content and/or applications on the Internet is also an Internet user.

Application of the Model Framework

64. Article 1 of the Model first defines network neutrality and subsequently explains the aim of this principle. In essence, network neutrality is a non-discrimination principle which applies to the transmission of Internet traffic.

65. According to this principle, all Internet traffic is to be transmitted equally and without undue discrimination, restriction or interference, regardless of the type or content of the traffic and regardless of the identity of its sender or recipient.

66. Since the goal of the net neutrality principle is to ensure that Internet traffic shall be treated without undue restriction, interference or discrimination, the format of article 10 ECHR lends itself very well to be transposed into a regulatory framework guaranteeing network neutrality. For this reason, article 2 of the Model contains the familiar formula of "no interference unless necessary and proportionate for a legitimate aim". This article should be applied according to the following five-step test:

67. First, it should be established whether or not an interference, restriction or discrimination has occurred. With respect to net neutrality this means that there is no interference if an ITM measure is fully application-agnostic, such as best-effort FIFO routing. Any ITM practice deviating from an application-agnostic approach should be deemed as an interference, restriction or discrimination.

68. The second step consists in determining whether the given ITM measure is prescribed by the agreement between the ISP and its subscriber (or another ISP, in the case of transit). If the agreement does not provide a sufficiently foreseeable ground for the ITM, the measure is illegal. If the ITM is prescribed by the agreement, we proceed to step three.

69. The third step consists in scrutinising whether the measure is justified by a legitimate aim or not. The purpose of the ITM measure must correspond with at least one of the legitimate aims, which are listed exhaustively in article 2, indents *a* to *e*.

70. The fourth step consists in determining if the measure is necessary in an open, end-to-end network. Can't the problem be properly solved at the edges? If there is no valid reason to implement a centralised measure to solve a specific problem, then the measure is not consistent with the network neutrality principle.

71. The fifth step consists in assessing the proportionality of the ITM measure. Notably, it should be evaluated whether the benefit brought by the specific measure exceeds its possible disadvantages

and whether it is possible to utilise a different, less discriminatory and possibly more efficient[97] measure in order to achieve the same purpose.

72. Similar to the way the ECtHR leaves a wider or smaller margin of appreciation to member states in certain situations, courts and regulatory authorities can leave a wider or smaller margin for ISPs to decide which ITM measures are necessary and proportionate. When competition is strong, switching is easy and transparency is optimal, courts and regulators can leave a wider margin of appreciation to ISPs. When the technical community is divided with regard to the discriminatory nature of a particular ITM measure, or its efficiency or proportionality, the margin of appreciation can be left wider as well. [98]

73. Article 2 delineates a limited number of legitimate aims for interferences. In accordance with indent *a*, an ISP is permitted to comply with a specific legislative provision or a court order prescribing an interference.

74. Indent *b* provides that an interference may be justified if necessary to safeguard the integrity and security of the network, services and Internet users' terminal equipment, for instance in order to block (D)DOS traffic or the proliferation of malware.

75. Further, indent *c* allows ISPs to implement measures restricting the transmission of unsolicited electronic communications for direct marketing purposes, commonly referred to as "spam".[99] Although the problem of spam can also be dealt with at the 'edges' of the networks, e.g. by filtering at the mail server level, it might be considered inefficient if all spam traffic, which is said

---

97 Port blocking can serve as an example of a measure that seems not quite efficient and would therefore quickly fail the net neutrality 'test' if there is another, more efficient measure available. E.g. the Broadband Internet Technical Advisory Group (BITAG) has highlighted that the common practice of "port blocking" – i.e. the practice of an ISP identifying Internet traffic by its port number and blocking it from reaching its destination – "can cause applications to "break" by preventing applications from using the ports they were designed to use" and in general "does not cause applications to vanish from the Internet, but rather induces a cat-and-mouse game whereby application development becomes increasingly complex to evade blocked ports". See: Cooper A., Limiting the Use of Port Blocking Advances Internet Neutrality, 20 August, 2013; BITAG, *Port Blocking, A Uniform Agreement Report*, August 2013.

98 As the state of the art evolves, it may at some point become clear that a certain application-specific measure which previously was broadly considered necessary and proportionate, gradually becomes inefficient and disproportionate by comparison to new measures, particularly if those measures are (more) application-agnostic. Therefore, it may be argued that the margin of appreciation becomes smaller when discriminatory ITM measures become more outdated in the light of newer, more efficient and/or more application-agnostic measures. We can imagine a 'cycle' where the same application-specific measure is first clearly necessary and proportionate, then gradually devolves and becomes less efficient at achieving its purpose compared to the state of the art, to a point where the measure is merely acceptable under the margin of appreciation for ISPs, while finally becoming unacceptable and disproportionate in the light of the development of newer and less discriminatory alternatives.

99 It should be noted that sending spam is illegal in most European jurisdictions. See: Directive 2002/58/EC (known as the e-Privacy Directive), article 13. The prohibition to transmit spam does not, however, apply to ISPs transmitting traffic of end-users as "mere conduits", but rather applies to the end-users themselves.

to constitute about 70-80 % of all e-mail traffic,[100] is first delivered to the end-point, taking up network capacity in the process, only to be discarded immediately after delivery. Therefore, filtering illegal spam at the network level forms a legitimate purpose. However, since filtering techniques always carry a risk of over-blocking, the model requires the consent of the receiving subscriber in order to put in place spam filtering at the network level (which may be less granular and less precise, compared with application-level filtering). In addition, although consent of the sending subscriber to filter outgoing spam is not necessary (indeed, it seems unlikely that a spammer would ever express it), article 2(c) requires that the least restrictive and least discriminatory method that is still sufficiently effective, be used.

76. In addition, article 2, indent *d* allows subscribers to request the adoption of certain application-specific ITM measures by the ISP. For example, this may involve Internet access services where the ISP is explicitly requested to filter out material that the subscriber objects to for religious reasons, or that is not deemed as suitable for children. Such filtering measures can also be performed at the edges, but if the Internet user prefers that the ISP takes care of this task, and the ISP offers this functionality, this should be allowed. It is also conceivable that certain Internet users may wish to prioritise traffic relating to certain favourite applications. The implementation of such an option in a way that leaves the Internet user in sufficiently direct control over what applications get priority and when – *i.e*. not by picking a plan that is set for the entire contract term – would be in accordance with the model. ISPs and their commercial partners may not, however, provide any monetary or other incentives (such as discounts or free items) for Internet users to accept or request discriminatory ITM measures.

77. It should be noted that article 2(d) does not encompass article 2(c), for their precise application differs. Article 2(c) foresees and permits a more active role of the ISP in preventing the transmission of unsolicited communications exclusively pertaining to "direct marketing purposes," requiring only the subscriber's prior consent to this type of filtering measure, and this only relates to the situation where the subscriber is the e-mail recipient. On the other hand, art. 2(d) requires "an explicit request from the subscriber" to legitimise any other forms of application-specific forms of traffic management. Given the fact that spam is an important problem on the Internet (as previously noted), it should be considered legitimate to ascribe a more active role to ISPs to combat this issue. To delineate the difference between the concepts of 'prior consent' and 'explicit request' within this context, we may consider that prior consent for spam-restricting measures may be given by the (mere) acceptance of general terms and conditions, whereas actively applying settings in a digital

[100] See: Internet Society, *Combating Spam: Policy, Technical and Industry Approaches*, 11 October 2012.

interface (e.g. in the router control panel or ticking a box in an online ordering process) could be said to constitute an 'explicit request'.

78. Lastly, it should be noted that, in the event of temporary and exceptional network congestion, it may be necessary to implement certain application-specific measures, such as prioritising traffic pertaining to real-time applications that are particularly sensitive to delay and jitter, such as (video) calling or gaming, over less time-sensitive applications, such as file sharing and e-mail. Indent e of article 2 leaves room for such interferences, but as it explicitly underlines: application-agnostic measures should be used if they are sufficiently effective in achieving the legitimate aim, whereas application-specific measures can only be justified if they prove more effective and/or efficient than any available application-agnostic alternatives.

79. As highlighted by network neutrality scholar Barbara van Schewick, application agnosticism requires ISPs to treat like traffic alike and bans discrimination targeting specific applications, content, services, and uses or classes of applications that share some common characteristic[101]. An example of application-agnostic ITM would be to allocate a larger portion of the available bandwidth in times of congestion, to those end-users having paid a higher fee for receiving a higher bandwidth.

80. This approach arguably "strikes the best balance between social benefits and social costs" because, contrary to application-specific discrimination, it does not interfere with end-users' decisions pertaining to what applications, content and services they utilise and how. In fact, it impedes to unduly discriminate data flows while allowing ISPs to differentiate their product and pricing offers regardless of the characteristics of a specific application (or class of applications), service, content or use. Hence, such an approach ascribes the responsibility to differentiate services to the end-users, not to the ISP, thus empowering individuals and fostering the circulation of innovation.

81. Indeed, application-agnostic traffic management seems particularly beneficial to foster a pluralistic online landscape and safeguard Internet-users' freedom to impart and receive information and ideas without undue interference. To this latter extent it must be noted that, in order to safeguard the key importance of freedom of expression as well as the diversity of the media landscape, as essential preconditions for a functioning democracy, the ECtHR has explicitly recognised the existence of positive obligations on Council of Europe members.[102]

---

[101] See: Van Schewick B., *Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like, op. cit.*, p. 40.

[102] Notably, in Özgür Gündem v. Turkey, the ECtHR has recalled that the "[g]enuine, effective exercise of [the] freedom [of expression] does not depend merely on the State's duty not to interfere, but may require positive measures of protection, even in the sphere of relations between individuals" See: Özgür Gündem v. Turkey, n°. 23144/93, § 43,

82. For these reasons, exceptional and temporary network congestion should primarily be mitigated by application-agnostic measures, and application-specific measure should only be employed when application-agnostic measures are insufficiently effective.

83. Importantly, article 2 gives no room for 'pay-for-priority' business models on the Internet. The mere fact that some entities may be willing to pay ISPs for implementing certain discriminations, restrictions or interferences, such as prioritising, throttling or blocking specific Internet traffic, does not constitute a legitimate aim for such interferences.

84. In accordance with article 3, the network neutrality principle should apply to both wired and wireless forms of Internet access services, regardless of the technology used to transmit signals (e.g. Ethernet, WiFi, or HDPA).

85. Pursuant to article 4, the network neutrality principle need not apply to specialised services, which may utilise the Internet Protocol, but which are offered on closed networks which are not part of the Internet and utilise strict access control. Examples of such services include certain IP-TV and VoIP services, often offered as a part of a 'triple play' package, where the subscriber of Internet access service also receives a 'set-top' box and digital home phones. We can also imagine certain e-health applications and other types of applications that have particularly high security requirements (a good rule of thumb is that anything connected to the Internet can be "hacked"), a high sensitivity to latency and jitter and a sufficiently high value to justify investments in closed networks providing specialised services besides the open Internet.[103] Pay-for-priority models in IP-based networks are therefore not banned *in toto*, as they can be realised through specialised services However, specialised services must not be offered in such a way that would degrade the quality of Internet access services below satisfactory levels and, if capacity is shared between Internet access services and specialised services, the ISP must clearly state this and the criteria whereby this sharing takes place. To this extent, regulatory authorities have the ability to set minimum requirements for the quality of Internet access services.

86. In accordance with article 5 of the Model, all Internet users have the right to a public IP address. A public IP address enables Internet users to be more than passive consumers of online

---

(2000-III). The pivotal importance of a pluralistic media landscape has been highlighted by the ECtHR in several occasions. See, *e.g.*: Informationsverein Lentia and others v. Austria, n° 13914/88; 15041/89; 15717/89; 15779/89; 17207/90 (1993); and the Observer and Guardian v. the United Kingdom, n° 13585/88 (1991).

[103] In the future we may expect to see less IP-TV and VoIP services offered as specialised services, because many Internet access services now offer sufficient bandwidth to enable on demand real-time streaming of 1080p resolution HD content (content distribution networks are helpful here as well), and Skype, Vonage and other Internet-based VoIP-applications normally have better sound quality than PSTN phone lines, while their quality can be considered comparable to specialised VoIP-services, unless they are being blocked or throttled, or if there is an exceptionally high level of congestion.

content and applications, but to be equal participants in the exchange of ideas, thoughts, information, services and applications online. This requirement can be expected to speed up adoption of IPv6 and reduce adoption of carrier-grade NAT, which may determine a variety of problems such as transforming 'big routers in big firewalls' .

87. Article 6 requires that any technique to inspect or analyse Internet traffic shall be limited to header information by default, and be reviewed by the relevant data protection authority if the contents of traffic are inspected or analysed.

88. Article 7 poses an obligation on ISPs to provide clear information about their traffic management policies. In order to provide the required transparency and information for users to base their choices for particular Internet access services on, ISPs must advertise the minimum bandwidth allocated to the Internet access service of the subscriber during the peak congestion levels on the ISPs network. This may be in addition to the theoretical maximum bandwidth levels which most ISPs currently advertise with.

89. Article 8 provides that regulatory authorities should have sufficient means and legal powers to effectively enforce net neutrality. The competent authority must regularly monitor and report on the compliance with net neutrality. The report by BEREC on traffic management practices could serve as a basis for such reporting, while the Model additionally prescribes that regulatory authorities must be properly equipped to assess net neutrality from a human rights perspective.

90. In this respect, it must be noted that, although existing European telecommunications regulation explicitly and consistently underlines the importance of human rights considerations with respect to telecommunications policy and its enforcement,[104] national telecoms regulators have considered themselves to lack competence to intervene in order to maximize the fundamental rights value of the Internet.[105] This points to a responsibility for legislators to grant regulators such competence.

91. Lastly, article 8(b) of the Model grants Internet users the right to file net neutrality infringement complaints with the regulatory authority as well as the competent court.

---

[104] Art. 3Bis of the Framework Directive.

[105] BEREC Response to the European Commission"s consultation on the open Internet and net neutrality in Europe 30 September 2010, para 4.5.

IV. Appendix - DRAFT Recommendation of the Committee of Ministers to member states on measures to safeguard network neutrality

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve greater unity between its members for the purpose of safeguarding and realising the ideals and principles which are their common heritage;

Recalling that States Parties to the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights – ETS No. 5) have undertaken to secure to everyone within their jurisdiction the human rights and fundamental freedoms defined in the Convention;

Recalling the 2010 Committee of Ministers Declaration of the Committee of Ministers on network neutrality, according to which electronic communication networks have become basic tools for the free exchange of ideas and information and, for this reason, users should have the greatest possible access to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice;

Recalling the 2003 Committee of Ministers Declaration on freedom of communication on the Internet, according to which Member states should foster and encourage access for all to Internet communication and information services on a non-discriminatory basis at an affordable price. Furthermore, the active participation of the public, for example by setting up and running individual websites, should not be subject to any licensing or other requirements having a similar effect;

Recalling Recommendation Rec(2007)11 of the Committee of Ministers to member states on promoting freedom of expression and information in the new information and communications environment, according to which member states, the private sector and civil society are encouraged to develop common standards and strategies to promote transparency and the provision of information, guidance and assistance to the individual users of technologies and services concerning, inter alia, the blocking of access to and filtering of content and services with regard to the right to receive and impart information;

Underlining the important role played by Internet Service Providers in delivering key services for the Internet user and stressing the importance of users' safety and their right to privacy and freedom of expression and, in this connection, the importance for the providers to be aware of the human rights impact that their activities can have;

Recognising the crucial contribution of the media in fostering public debate, political pluralism and awareness of diverse opinions;

Reaffirming that media pluralism and diversity of media content are essential for the functioning of a democratic society and are the corollaries of the fundamental right to freedom of expression and information as guaranteed by Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms;

Recalling Recommendation CM/Rec(2007)2 of the Committee of Ministers to member states on media pluralism and diversity of media content, according to which Member states should seek to ensure that a sufficient variety of media outlets provided by a range of different owners, both private and public, is available to the public, taking into account the characteristics of the media market, notably the specific commercial and competition aspects;

Aware at the same time of the need to balance freedom of expression and information with other legitimate rights and interests, in accordance with Article 10, paragraph 2 of the Convention for the Protection of Human Rights and Fundamental Freedoms;

Noting that information and communication technologies (ICTs) can, on the one hand, significantly enhance the exercise of human rights and fundamental freedoms, such as the right to freedom of expression, information and communication, the right to education, the right to assembly, and the right to free elections, while, on the other hand, they may adversely affect these and other rights, freedoms and values, such as the respect for private life and secrecy of correspondence, the dignity of human beings and even the right to life;

Noting that information and communication technologies (ICTs) allow the collection and processing on a large scale of data, including personal data, in both the private and public sectors; noting that ICTs are used for a wide range of purposes including uses for services widely accepted and valued by society, consumers and the economy; noting at the same time that continuous development of convergent technologies poses new challenges as regards collection and further processing of data;

Aware that communication using new information and communication technologies and services must respect the right to privacy as guaranteed by Article 8 of the European Convention on Human Rights and by the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), and as elaborated by Recommendation No. R (99) 5 of the Committee of Ministers to ember states on the protection of privacy on the Internet;

Convinced that access to and the capacity and ability to use the Internet should be regarded as indispensable for the full exercise and enjoyment of human rights and fundamental freedoms in the information society;

Aware that the media landscape is rapidly changing and that the Internet is playing an increasingly important role in providing and promoting diverse sources of information to the public, including user-generated content;

Recalling the Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, which highlights the public service value of the Internet, understood as people's significant reliance on the Internet as an essential tool for their everyday activities (communication, information, knowledge, commercial transactions) and the resulting legitimate expectation that Internet services be accessible and affordable, secure, reliable and ongoing

Recommends that, having regard to the model framework on network neutrality in the appendix to this recommendation, the governments of member states, in co-operation, where appropriate, with all relevant stakeholders, take all necessary measures to safeguard the principle of network neutrality.

Recommended Model Framework on Network Neutrality

1) Network neutrality is the principle according to which Internet traffic shall be treated equally, without discrimination, restriction or interference regardless of its sender, recipient, type or content, so that Internet users' freedom of choice is not restricted by favouring or disfavouring the transmission of Internet traffic associated with particular content, services, applications, or devices.

2) In accordance with the network neutrality principle, Internet service providers shall refrain from discriminating, restricting, or otherwise interfering with the transmission of Internet traffic, unless such interference is strictly necessary and proportionate to:

a) give effect to a legislative provision or court order;

b) preserve the integrity and security of the network, services and the Internet users' terminal equipment;

c) prevent the transmission of unsolicited communications for direct marketing purposes to Internet users who have given their prior consent to such restrictive measures;

d) comply with an explicit request from the subscriber, provided that this request is given freely and is not incentivised by the Internet service provider or its commercial partners;

e) mitigate the effects of temporary and exceptional network congestion, primarily by means of application-agnostic measures or, when these measures do not prove efficient, by means of application-specific measures.

3) The network neutrality principle shall apply to all Internet access services and Internet transit services offered by ISPs, regardless of the underlying technology used to transmit signals.

4) The network neutrality principle need not apply to specialised services. Internet service providers should be allowed to offer specialised services in addition to Internet access service, provided that such offerings are not to the detriment of Internet access services, or their performance, affordability, or quality. Offerings to deliver specialised services should be provided on a non-discriminatory basis and their adoption by Internet users should be voluntary.

5) Subscribers of Internet access service have the right to receive and use a public and globally unique Internet address.

6) Any techniques to inspect or analyse Internet traffic shall be in accordance with privacy and data protection legislation. By default, such techniques should only examine header information. The use of any technique which inspects or analyses the content of communications should be reviewed by the relevant national data protection authority to assess compliance with the applicable privacy and data protection obligations.

7) Internet service providers shall provide intelligible and transparent information with regard to their traffic management practices and usage polices, notably with regard to the coexistence of Internet access service and specialised services. When network capacity is shared between Internet access services and specialised services, the criteria whereby network capacity is shared, shall be clearly stated.

8) The competent national regulatory authority shall:

a) be mandated to regularly monitor and report on Internet traffic management practices and usage polices, in order to ensure network neutrality, evaluate the potential impact of the aforementioned practices and policies on fundamental rights, and ensure the provision of a sufficient quality of service and the allocation of a satisfactory level of network capacity to the Internet. Reporting should be done in an open and transparent fashion and reports shall be made freely available to the public;

b) put in place appropriate, clear, open and efficient procedures aimed at addressing network neutrality complaints. To this end, all Internet users shall be entitled to make use of such complaint procedures in front of the relevant authority;

c) respond to the complaints within a reasonable time and be able to use necessary measures in order to sanction the breach of the network neutrality principle.

d) This authority must have the necessary resources to undertake the aforementioned duties in a timely and effective manner.

9) Definitions

a) The “Internet” is the publicly accessible electronic communications network of networks that use the Internet Protocol for communication with endpoints reachable, directly or through network address translation, via a globally unique Internet address.

b) The expression “Internet service provider” refers to any legal person that offers Internet access service to the public or Internet transit service to another ISP.

c) The expression “Internet access service” refers to a publicly available electronic communications service that provides connectivity to the Internet, and thereby provides the ability to the subscriber or Internet user to receive and impart data from and to the Internet, irrespective of the underlying technology used to transmit signals.

d) The expression “Internet transit service” refers to the electronic communications service that provides Internet connectivity between Internet service providers.

e) The expression “Internet traffic” refers to any flow of data packets transmitted through the Internet, regardless of the application or device that generated it.

f) The expression “specialised services” refers to electronic communications services that are provided and operated within closed electronic communications networks using the Internet Protocol, but not being part of the Internet. The expression “closed electronic communications networks” refers to networks that rely on strict admission control.

g) The expression “application-agnostic” refers to Internet traffic management practices, measures and techniques that do not depend on the characteristics of specific applications, content, services, devices and uses.

h) The expression “subscriber” refers to the natural or legal person who has entered into an agreement with an Internet service provider to receive Internet access service.

i) The expression “Internet user” refers to the natural or legal person who is using Internet access service, and in that capacity has the freedom to impart and receive information, and to use or offer applications and services through devices of their choice. The Internet user may be the subscriber, or any person to whom the subscriber has granted the right to use the Internet access service s/he receives. Any legal person offering content and/or applications on the Internet is also an Internet user.

V. Glossary

Application-agnosticism: the establishment of Internet traffic management practices, measures and techniques that do not depend on the characteristics of specific applications, content, services, devices and uses.

Electronic communications network: a transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.

Data flow: a set of packets traversing a network element. It may consist of the packets from a single application session, or it may be an aggregation comprising the combined data traffic from a number of application sessions.

Data packet: a data packet is a unit of digital information that travels along a given network path on 'packet-switched' networks. An example of a data packet is an IP packet, containing data in a 'package' suitable for transfer over networks utilising the Internet Protocol. A data packet is structured in a 'payload' which is a set of raw data it contains, and a header that carries metadata, including (routing) information, such as destination and origin.

End-user: see **Internet user.**

Internet: the publicly accessible electronic communications network of networks that use the Internet Protocol for communication with endpoints reachable, directly or through network address translation, via a globally unique Internet address.

Internet access service: the publicly available electronic communications service that provides connectivity to the Internet, and thereby provides the ability to the subscriber or Internet user to receive and impart data from and to the Internet, irrespective of the underlying technology used to transmit signals.

Internet protocol (IP): the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Using the Internet Protocol entails the assignment of IP addresses.

Internet service provider (ISP): any legal person that offers Internet access service to the public or Internet transit service to another ISP.

Internet traffic: one or more data flow(s) transmitted through the Internet, regardless of the application or device that generated it.

Internet traffic delivery: the ordering and transmission of data-packets from one end-point, identified with a specific IP address, to another.

Internet traffic management (ITM): all technical means used to process through the network traffic sent or received by end users, including both application-specific and application-agnostic traffic management.

Internet transit service: the electronic communications service that provides Internet connectivity between Internet service providers.

Internet user: any natural or legal person who is using Internet access service, and in that capacity has the freedom to impart and receive information, and to use or offer applications and services through devices of their choice. The Internet user may be the subscriber, or any person to whom the subscriber has granted the right to use the Internet access service s/he receives. Any legal person offering content and/or applications on the Internet is also an Internet user.

IP Address: a numerical label assigned to each device (e.g., computer, printer, router) participating in an IP-based network.

IP-based network: a packet-switched communication network utilising the Internet Protocol.

Network element: any component of an inter-network, which directly handles data packets. Network elements include routers, sub-networks, and end-node operating systems.

Network neutrality is the principle according to which Internet traffic shall be treated equally, without discrimination, restriction or interference regardless of its sender, recipient, type or content, so that end-users' freedom of choice is not restricted by favouring or disfavouring the transmission of Internet traffic associated with particular content, services, applications, or devices.

Packet-switched network: a communications network in which digital information is broken down in 'data packets' and routed from source to destination via switches and routers.

Specialised services: sometimes referred as "managed services", they are electronic communications services that are provided and operated within closed electronic communications networks using the

Internet Protocol, but not being part of the Internet. The expression “closed electronic communications networks” refers to networks that rely on strict admission control.

Subscriber: a natural or legal person who has entered into an agreement with an Internet service provider to receive Internet access service.

VI. List of abbreviations

ARCEP	Autorité de régulation des communications électroniques et des postes.
Art.	Article.
AS	Autonomous System.
ASQ	Assured service quality.
BEREC	Body of European Regulators for Electronic Communications.
BSP	Broadband service provider.
CAP	Content and application provider.
CDN	Content Delivery Network.
CNNum	Conseil national du numérique.
(D)DoS(-attack)	(Distributed) denial of service (attack).
DPI	Deep packet inspection.
ECHR	European Convention on Human Rights.
ECtHR	European Court of Human Rights.
ETNO	The European Telecommunications Network Operators' Association.
FCC	Federal Communications Commission of the United States of America.
IANA	Internet Assigned Names and Numbers Association.
IETF	Internet Engineering Task Force.
IP	Internet Protocol.
ISP	Internet service provider.
ITM	Internet traffic management.
LAN	Local area network.
ISOC	Internet Society
NAT	Network address translation.
NRA	National regulatory authority (in the field of telecommunications).
QoS	Quality of Service.
RFC	Request for Comments.

RST(-packet)	Reset packet (as intended in RFC 793).
TEU	Treaty on European Union.
TLD	Top Level Domain.
VoIP	Voice over IP, or voice over the Internet (Protocol).

VII. References

ARCEP, *Report to Parliament and the Government on Net Neutrality*, September 2012, p. 16, available at http://www.arcep.fr/uploads/tx_gspublication/rapport-parlement-net-neutrality-sept2012-ENG.pdf.

Balkin J., *Digital Speech and Democratic culture: a Theory of Freedom of Expression for the Information Society*, New York University Law Review, Vol 79:1, available at http://www.yale.edu/lawweb/jbalkin/telecom/digitalspeechanddemocraticculture.pdf.

Belli L., *Council of Europe Multi-Stakeholder Dialogue on Network Neutrality and Human Rights, Outcome Paper*, June 2013.

Belli L. & Van Bergen M., *A Discourse-Principle Approach to Network Neutrality: A Model Framework and its Application*, in Belli L. & De Filippi P. (ed.), The Value of Network Neutrality for the Internet of Tomorrow, Report of the Dynamic Coalition on Network Neutrality, 2013, available at http://nebula.wsimg.com/a0d2191d5788b8177915108786bfba7a?AccessKeyId=B45063449B96D27B8F85&disposition=0.

Bendrath R., *Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection*, March 2009, available at http://userpage.fu-berlin.de/bendrath/Paper_Ralf-Bendrath_DPI_v1-5.pdf.

Benkler Y., *The Wealth of Networks*, Yale University Press, 2006, available at http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf.

BEREC, *A view of traffic management and other practices resulting in restrictions to the open Internet in Europe*, 29 May 2012, availabl at https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf.

BEREC, *BEREC's comments on the ETNO proposal for ITU/WCIT or similar initiatives along these lines*, BoR (12) 120 rev.1, 14 November 2012, available at http://berec.europa.eu/files/document_register_store/2012/11/BoR(12)120rev.1_BEREC_Statement_on_ITR_2012.11.14.pdf.

BEREC, *BEREC Guidelines for quality of service in the scope of net neutrality*, BoR (12) 131, 26 November 2012.

BEREC 2012, *Overview of BEREC's approach to net neutrality*, BoR (12) 140, http://berec.europa.eu/files/document_register_store/2012/12/BoR_(12)_140_Overview+of+BEREC+approach+to+NN_2012.11.27.pdf.

BEREC, *Differentiation practices and related competition issues in the scope of Net Neutrality*, May 2012, available at http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/1094-berec-report-on-differentiation-practices-and-related-competition-issues-in-the-scope-of-net-neutrality.

BEREC Response to the European Commission‟s consultation on the open Internet and net neutrality in Europe 30 September 2010, available at http://www.irg.eu/streaming/BoR%20(10)%2042%20BEREC%20response_ECconsultation_Net%20neutrality_final.pdf?contentId=546969&field=ATTACHED_FILE

Berkman Center for Internet & Society at Harvard Law School, *Roadmap for Open ICT Ecosystems*, 2005, available at http://cyber.law.harvard.edu/epolicy/roadmap.pdf.

Berkman Center for Internet & Society at Harvard University, *Next Generation Connectivity: A review of broadband Internet transitions and policy from around the world*, February 2010, available at http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Berkman_Center_Broadband_Final_Report_15Feb2010.pdf.

Berners-Lee T., *Net Neutrality: This is serious*, 2006-06-2, available at http://dig.csail.mit.edu/breadcrumbs/node/144.

Berners Lee T., *Long live the web,* Scientific American November 22 2010, available at http://www.scientificamerican.com/article.cfm?id=long-live-the-web

BITAG, *Port Blocking, A Uniform Agreement Report*, August 2013, available at http://www.bitag.org/documents/Port-Blocking.pdf.

Chirico F., Van der Haar I. and Larouche P., *Network Neutrality in the EU*, TILEC Discussion Paper, 2007, available at http://arno.uvt.nl/show.cgi?fid=122425.

Christopher T. Marsden, *Net Neutrality: Past Policy, Present Proposals, Future Regulation?* in Belli L. & De Filippi P. (ed.), The Value of Network Neutrality for the Internet of Tomorrow, Report of the Dynamic Coalition on Network Neutrality, 2013.

Cisco, *Cisco Visual Networking Index: Forecast and Methodology, 2012–2017*, May 29, 2013, available at http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf.

Clark D.D. and &Marjory S. Blumenthal M.S., *The end-to-end argument and application design: the role of trust*, in Federal Communications Law Journal, vol. 63, n°357, 2011.

Cooper A., *Limiting the Use of Port Blocking Advances Internet Neutrality*, 20 August, 2013, available at https://www.cdt.org/blogs/alissa-cooper/2008limiting-use-port-blocking-advances-internet-neutrality.

Council of Europe, *2010 Declaration of the Committee of Ministers on Network Neutrality*, available at https://wcd.coe.int/ViewDoc.jsp?id=1678287&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

Council of Europe, *Internet Governance, Council of Europe Strategy 2012-2015*, CM(2011)175 final, 15 March 2012, paragraph I.8.e, available at https://wcd.coe.int/ViewDoc.jsp?id=1919461.

Council of Europe, *Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet*, available at https://wcd.coe.int/ViewDoc.jsp?id=1207291.

CPB *response of 23 September 2010 to the public consultation on Internet and net neutrality*, available at http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/net_neutrality/comments/10academics_policy_analysts_etc/cpb_netherlands_bureau_for_economic_policy_analysis.pdf.

Daly A., *The legality of deep packet inspection*, in International Journal of Communications Law and Policy, 2011, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1628024.

DC NN Coalition mailing list archives, available at http://mailman.edri.org/pipermail/nncoalition/.

ETICS Deliverable D3.5, 'Final Business Models Analysis', available at https://bscw.ict-etics.eu/pub/bscw.cgi/d45665/D3.5_final_v1.0.pdf.

ETICS Deliverable D4.3: 'Revision of ETICS Architecture and Functional Entities', available at http://ec.europa.eu/information_society/apps/projects/logos/7/248567/080/deliverables/001_ETICSD43v10.pdf.

ETNO paper on Contribution to WCIT ITRs Proposal to Address New Internet Ecosystem, available at http://www.etno.eu/datas/itu-matters/etno-ip-interconnection.pdf.

European Data Protection Supervisor, *Opinion on net neutrality, traffic management and the protection of privacy and personal data*, 7 October 2011, p. 8, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-10-07_Net_neutrality_EN.pdf.

Faratin P. et al. *The Growing Complexity of Internet Interconnection*, in Communications & Strategies n° 72, 4th quarter 2008, available at http://www.akamai.com/dl/technical_publications/growing_complexity_of_internet.pdf.

FCC 10-201, *Report and order on the open Internet 2010*, available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf.

Felten B., *There's No Economic Imperative to Reconsider an Open Internet*, April 3, 2013, available at http://ssrn.com/abstract=2244335.

French Constitutional Council, Decision No. 2009-580DC of the 10th of June 2009.

Gallie W.B., *Essentially Contested Concepts*, in Proceedings of the Aristotelian Society, New Series Vol.56, 1956.

High Level Group on Media Freedom and Pluralism, *A free and pluralistic media to sustain European democracy*, January 2013, available at https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/HLG%20Final%20Report.pdf.

Huston G. APNIC, RIPE 65, September 2012, *The Concept of Quality of Service in the Internet*, available at https://ripe65.ripe.net/presentations/67-2012-09-25-qos.pdf.

Internet Architecture Board, *Affirmation of the Modern Paradigm for Standards*, Request for Comments: 6852, January 2013, available at http://tools.ietf.org/html/rfc6852.

Internet Society, *Combating Spam: Policy, Technical and Industry Approaches*, 11 October 2012, available at http://www.internetsociety.org/sites/default/files/Combating-Spam.pdf.

Kahin B. & Keller J., *Public Access to the Internet*, MIT Press, 1995.

Kearney A.T., *A Viable Future Model for the Internet*, 2011, p. 7, available at http://www.atkearney.com/documents/10192/4b98dac5-0c99-4439-9292-72bfcd7a6dd1.

Kocsis V. and Jarst Weda J, *The innovation-enhancing effects of network neutrality*, study commissioned by the Dutch Ministry of Economic Affairs, Amsterdam, 12 June 2013, available at http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2013/08/22/innovatieversterkende-werking-van-netneutraliteit/seo-report-2013-33-network-neutrality.pdf.

KPN Investor Day, London 10 May 2011, available at http://pulse.companywebcast.nl/playerv1_0/default.aspx?id=12193&bb=true&swf=true.

La Rue F., *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 16 May 2011, nr. A/HRC/17/27, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

La Quadrature du Net, *Neelie Kroes Pushing Telcos' Agenda to End Net Neutrality,* 30 August 2013, available at http://www.laquadrature.net/en/neelie-kroes-pushing-telcos-agenda-to-end-net-neutrality.

Lessig L. & McChesney R.W., *No Tolls on the Internet,* Washington Post, 8 June 2006, available at: http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/AR2006060702108.html.

Licklider J.C.R*., IRE Transactions on Human Factors in Electronics*, volume HFE-1, pages 4-11, March 1960, http://groups.csail.mit.edu/medg/people/psz/Licklider.html.

McNamee J., *The Slide from "Self-regulation" to Corporate Censorship*, 2011, available at http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf.

Marsden C.T., *Net Neutrality Towards a Co-regulatory Solution*, Bloomsbury Academic, 2010.

Marsden C.T., *Question for IGF net neutrality coalition: Regarding specialised service*, 18 September, 2013, available at http://chrismarsden.blogspot.fr/2013/09/question-for-igf-net-neutrality.html.

Marsden C.T., University of Sussex, *(Pre)-history of European Network Neutrality and Human Rights*, Strasbourg, 29 May 2013, available at http://fr.slideshare.net/EXCCELessex/pre-history-of-european-network-neutrality-and-human-rights.

Network Working Group, Request for Comments: 1958, *Architectural Principles of the Internet*, June 1996, available at http://www.ietf.org/rfc/rfc1958.txt.

Network Working Group, *The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture, Request for Comments: 3724*, March 2004, available at http://www.ietf.org/rfc/rfc3724.txt.

OECD, *Communiqué on Principles for Internet Policy-Making*, 28-29 June 2011, available at http://www.oecd.org/internet/innovation/48289796.pdf.

OpenNet Initiative, Country Profiles, available at https://opennet.net/country-profiles.

Open Rights Group blog, *Orange UK blocking La Quadrature du Net*, February 15, 2012, available at http://www.openrightsgroup.org/blog/2012/orange-uk-blocking-la-quadrature-du-net.

Parsons C., *Literature Review of Deep Packet Inspection*, Prepared for the New Transparency Project's CyberSurveillance Workshop, version 4.1, 6 March 2011.

Plum Consulting, *The open internet – a platform for growth*, October 2011, available at http://www.channel4.com/media/documents/press/news/Plum_October2011_The_open_internet_-_a_platform_for_growth.pdf.

Radisys, DPI: *Deep Packet Inspection Motivations, Technology, and Approaches for Improving Broadband Service Provider ROI*, September 2010, p. 4, available at http://go.radisys.com/rs/radisys/images/paper-dpi-motivations.pdf.

Saltzer J.H., Reed D.P. & Clark D.D., *End-to-end arguments in system design*, in ACM Transactions on Computer Systems n°2, 1984.

Slater D. & Wu T., *Homes with Tails: What if You Could Own Your Internet Connection?* in *New America Foundation Wireless Future Program*, Working Paper #23, 2008, available at http://www.newamerica.net/files/nafmigration/HomesWithTails_wu_slater.pdf.

Sørensen F., Reply to the mailing-list of the Dynamic Coalition on Network Neutrality, 21 September 2013, available at http://mailman.edri.org/pipermail/nncoalition/.

Sørensen F., *10 myths about net neutrality*, March 2013, available at http://www.npt.no/aktuelt/nyheter/_attachment/6807?_ts=13da6dd5c75.

Statistics Netherlands, Reaction of Statistics Netherlands to the internet consultation of the European Commission, available at http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/net_neutrality/comments/10academics_policy_analysts_etc/cpb_netherlands_bureau_for_economic_policy_analysis.pdf.

TOR Project Blog, *A tale of new censors - Vodafone UK, T-Mobile UK, O2 UK, and T-Mobile USA*, 17 January 2012, available at https://blog.torproject.org/blog/tale-new-censors-vodafone-uk-t-mobile-uk-o2-uk-and-t-mobile-usa.

Van Schewick B., *Internet Architecture and Innovation*, MIT Press, 2010.

Williamson B., Black D. & Punton T., *The open internet – a platform for growth*, October 2011, available at http://www.channel4.com/media/documents/press/news/Plum_October2011_The_open_internet_-_a_platform_for_growth.pdf.

WIK-Consult, *Network operators and content providers: Who bears the cost?,* 9 September 2011, p. 75, available at http://ipv6.ppk.itb.ac.id/~dikshie/CCN/Incentives/SSRN-id1926768.pdf.

Wu T., *Network Neutrality, Broadband Discrimination*, in Journal of Telecommunications and High Technology Law, Vol. 2, p. 141, 2003, available at: http://ssrn.com/abstract=388863.

Zhu K., *Bringing Neutrality to Network Neutrality*, in Berkeley Technology Law Journal vol. 22, n° 615, 2007, available at https://secure.ocf.berkeley.edu/~step/White_Paper/Zhu.pdf.

Zittrain J., *The Future of the Internet and How to Stop It*, Yale University Press, 2008, available at http://futureoftheinternet.org/files/2013/06/ZittrainTheFutureoftheInternet.pdf.