The value of Network Neutrality for the Internet of Tomorrow

Luca Belli, Primavera de Filippi

The Value of Network Neutrality for the Internet of Tomorrow

The Value of Network Neutrality for the Internet of Tomorrow

Report of the Dynamic Coalition on Network Neutrality

Edited by Luca Belli & Primavera De Filippi

Preface by Marietje Schaake

TABLE OF CONTENTS

Foreword

A New Arrival in the IGF Family: The Dynamic Coalition on Network Neutrality

by Luca Belli

On 12 July 2013, the Secretariat of the United Nations' Internet Governance Forum (IGF) approved the creation of the Dynamic Coalition on Network Neutrality.

Along with a conspicuous number of workshops, dynamic coalitions represent the structural elements of the IGF. Both elements have a heterogeneous multi-stakeholder composition and are aimed at the discussion of "public policy issues related to key elements of Internet governance", as the IGF mandate suggests. (Tunis Agenda, para. 72.a)

On the one hand, IGF workshops are unique events which allow various stakeholders to jointly analyse "hot topics" or to examine progress that such issues have undertaken since the previous IGF. On the other hand, dynamic coalitions are supposed to evolve over the years in a lively fashion and represent an exceptional opportunity to build an enduring and collaborative policy-shaping effort.

The long-term nature of dynamic coalitions is probably better-suited in order fulfil one of the most forgotten subparagraphs of the IGF mandate, according to which the forum shall "[i]dentify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations". (Tunis Agenda, para. 72.g)

Indeed, IGF workshops are extremely circumscribed events and although the content of their discussion is usually extremely valuable, their 90-minute length does not allow them to generate political momentum around the issues they raise and confines workshops' debates to a conference-centre room and to a usually un-consulted report. *Au contraire*, dynamic-coalitions' activities are supposed to be much broader than a 90-minute-long meeting, which is rather a moment to share the work that has been achieved over the year, discuss it and envisage the next steps.

The Interest of Creating a Dynamic Coalition on Network Neutrality

"Network neutrality" is an appealing and multifaceted expression which encompasses several policy areas and may give rise to misinterpretations.

In view of the various approaches to this multi-faceted topic, it is important today to address the question of network neutrality through a multi-stakeholder approach. The purpose of the Network Neutrality Dynamic Coalition, therefore, is to provide a discussion arena aimed at allowing all interested stakeholders to jointly scrutinise the various nuances of the network-

neutrality debate so as to ultimately contribute to the circulation of best practices and the elaboration of well-advised policies and regulations.

The idea of a Dynamic Coalition on Network Neutrality was presented during Multi-Stakeholders Dialogue on Network Neutrality & and Human Rights, organised under the auspices of the Council of Europe. Many of the stakeholders involved in the event have immediately manifested their interest in the initiative, stressing the need to clarify the network neutrality debate and highlighting the interest of a platform aimed at promoting the dialogue on the matter.

An Action Plan

The Dynamic Coalition on Network Neutrality will provide a common platform involving a large variety of stakeholders in a cooperative analysis of the network neutrality debate. Beyond the website, which will provide basic information on the work done by the dynamic coalition (*e.g.* publications, events, etc.), the official mailing list of the coalition will allow all members and interested individuals to discuss in an open and interactive fashion.

The goal of the Dynamic Coalition will be to stimulate the exchange of ideas and disseminate information on current trends and policy developments pertaining to network neutrality. To this end, an annual report will be produced to provide an overview on Net Neutrality tendencies, policies and draft legislation.

To this end, the first Annual Report is dedicated to the relation between network neutrality and human rights and encompasses a selection of position papers that aim at elucidating such a crucial debate.

Lastly, the Dynamic Coalition has attempted to elaborate a "model framework" on network neutrality, which can be deemed as consistent with international human-rights standards. Such a model framework aims at providing guidance to national legislators and respond to the growing need for a network-neutrality regulation able to safeguard end-users' human rights and fundamental freedoms while fostering fair competition and freedom to innovate.

By all means, every interested stakeholder is welcome to join this collaborative effort. All information pertaining to the Dynamic Coalition can be found at networkneutrality.info

Preface

by Marietje Schaake

This report by the Dynamic Coalition on Network Neutrality is perfectly timed, shortly after Commissioner Kroes, in charge of Europe's Digital Agenda, presented her plans to create a single telecoms market in the European Union.

Commissioner Kroes' goal to harmonize the European telecoms markets is an important step towards the long overdue completion of the European Digital Single Market. However, the proposed clauses that are labelled 'net neutrality' in the regulation are cause for concern. This report can serve as an important basis for the many discussions on the issue of net neutrality which the European Parliament and many stakeholders will see in the coming months.

The internet was created with no other use in mind than the efficient transfer of information. Over the last 20 years the internet and information technology have developed at an extremely rapid pace, giving rise to huge economic and social benefits. The key driver of this unprecedented innovation has been that all information flows and services are treated equally, without discrimination, conform to the principle of net neutrality. This is the basic prerequisite for a free and open internet. Until recently the assumption was that competition and transparency would offer sufficient safeguards for internet users.

Through its open nature, the internet has become an increasingly important enabler of human rights. Especially freedom of expression, but also press freedom, access to information and freedom of association. The internet boosts several other important factors in our lives, such as economic, social and also political developments. In fact, it is hard to imagine a world without being connected anymore.

As a global economic force and a community of values, the EU has both an interest and a responsibility to become a global leader in the protection of digital freedoms. We need to counterbalance regimes or companies that seek to do irreversible damage to the open internet for short term political or economic gains and consequently put human rights under pressure. Leadership starts at home.

The importance of ensuring competition, innovation and access to information for the next decades, requires legal guarantees. The EU should therefore take the lead on actually enshrining net neutrality in law. This will require an approach that is ambitious, principled, and puts users first. The public value of the open internet is too often overlooked. Internet service providers (ISPs) have to treat all data equally, cannot block any content, must allow for fair competition on the internet. This would protect users from the abuse of power of major market players. Such measures should allow all internet users universal access to all online resources and services.

In the Netherlands net neutrality was enshrined in law in 2011 on the initiative of the social-liberal party D66 after a major telecoms provider spoke to shareholders about its throttling of the Voice over IP and messaging services that directly competed with its core business of selling text messages and calling minutes. Research by the board of European telecom regulators, BEREC, has shown that Dutch telecom providers are hardly the only ones guilty of these practices. Hundreds of millions of Europeans do not have access to all information or services online.

Practices such as throttling or blocking of data or the blocking of specific services such as Voice over IP (VoIP) are occurring widely and often require intrusive techniques such as deep packet inspection (DPI) in order for ISPs to identify and either prioritize or throttle certain data packets. The good news is that Commissioner Kroes' proposal puts an end to these practices, but the risk of deals between major market players is such, that net neutrality remains at risk.

We cannot understate the consequences of this proposal for the competitiveness of the European digital economy. By allowing so called Assured Quality Service provisions, in which companies can make deals with ISPs to provide faster internet at higher prices, the proposal can limit the possibilities for new players whose pockets are not as deep. This would stifle innovation. We already see that more and more internet service providers and content providers are making deals. We need to ensure that these deals do not hurt consumer choice or access to information in the long run. It is essential that major market players cannot abuse their power and that the public interest is not forgotten. When hospitals, libraries and universities cannot afford to pay for higher speeds they risk being crowded out. Rather net neutrality legislation should provide a level playing field on which the same conditions apply to all players. To give new services and innovative start-ups a fair chance, incumbents should not be favoured over newcomers in the market. Ultimately this leads to consumers paying too much.

The European Parliament now has a historic opportunity to get net neutrality right. For the EU to be able to credibly advocate digital freedoms abroad, we need to get our own house in order and guarantee an open and competitive internet. Implementing net neutrality legislation in the EU is not only important today, but will be increasingly essential tomorrow. In a legal vacuum, we risk a race to the bottom. This report will serve as a much needed stepping stone to avoid such a race to the bottom and have an informed debate about net neutrality in the European Parliament in coming months.

Introduction

Framing the Network Neutrality debate: a multi-stakeholder approach towards a policy blue-print

by Primavera De Filippi and Luca Belli

Network Neutrality (NN) refers to the principle whereby all electronic communication should be treated in a non-discriminatory way, regardless of their type, content, origin or destination. Originally seen as a network design principle (Wu, 2003), it is, nowadays, increasingly regarded as a normative principle (BEREC, 2012) aimed at ensuring that all Internet users be granted universal and non-discriminatory access to all legitimate online resources (content, services, or applications), along with the right to have their own resources universally available on the Internet.

Although only a few countries have enacted NN regulations, so far the establishment of an open and neutral Internet is regarded as a key driver for economic growth (World Bank, 2009). At the European level, the European Parliament (2012a, 2012b) has explicitly recognized the importance to enshrine the NN principle into legislation to promote the establishment of a European Digital Single Market. To this extent, the European Commission recently proposed a Regulation for a Single Telecoms Market (September 2013) aimed at securing NN by precluding Internet Service Providers (ISPs) from discriminating against specific services, content or applications - while nonetheless allowing them to enter into contractual agreements to provide certain content and applications providers (CAPs) with enhanced quality of service.

Beyond economic considerations, the establishment of an open and neutral Internet is also a precondition for the full enjoyment of human rights (CoE, 2011). In his paper, Luca Belli reflects on the relationship between "Network Neutrality and Human Rights". After introducing the concept of NN, the paper provides a general overview of the main discriminatory practices threatening NN, and their consequences on human rights. On the one hand, NN is constrained by the fact that national legislators can impose a series of limitations on users' access to online resources for the sake of public order or morality. ISPs can in fact be required to block access to infringing online material, as well as to filter online communications that either support or promote illegal activities. While this is generally justified on legitimate purposes, authoritarian regimes could also abuse their leeway in order to enforce censorship. On the other hand, the NN principle may be endangered by traffic management policies aimed at improving the quality of specific online services by giving higher priority to certain data flows. Indeed, according to some ISPs, the current increase in

Internet traffic justify the use of traffic management techniques in order to optimise bandwidth allocation. These techniques are therefore being employed by telecommunication carriers (especially mobile-Internet access providers) as a means to ensure a minimum quality of service, frequently blocking, filtering, throttling or prioritizing specific data flows. To the extent that they might result in packet discrimination, these practices might impinge upon users' right to receive and impart information, as well as the privacy of their communications.

The potential for the Internet to further fundamental human rights (such as freedom of expression, access to knowledge and democratic participation) ultimately depends upon the design of the network which - based on the end-to-end principle - enables users to freely choose (and run) specific services and applications, as well as to connect the devices that they consider the most appropriate to satisfy their needs. Yet, as illustrated by Andrew McDiarmid and Matthew Shears in "The Importance of Internet Neutrality to Protecting Human Rights Online", Internet's full potential can only be unleashed insofar as the network stays compatible with the NN principle. To preserve users' fundamental rights, the Internet must, indeed, remain *global* (allowing for communications to be distributed worldwide), *user-controlled* (as opposed to being controlled by the content or access provider), *decentralized* (with most services and applications running at the edges of the network), *open and competitiv*e (with relatively low barriers to entry). McDiarmid argues that, given the growing role that the Internet plays with regard to various facets of our life, States have the duty to intervene so as to ensure that the network design remains such as to promote the exercise of fundamental human rights.

Indeed, NN is nowadays regarded as a precondition for users to fully enjoy their fundamental freedom of expression (OECD, 2005; CoE, 2011), defined by the Universal Declaration of Human Rights as "the right to freedom of opinion and expression; [including] freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

To this latter extent, Maria Löblich and Francesca Musiani have analysed the impact of NN on democratic participation in their paper on "Net Neutrality from a Public Sphere Perspective", through Peter Dahlgren's three-dimensional framework. Dahlgren (1995) distinguishes between the *structural dimension* of public sphere, referring to the various media available for the public to communicate, the *representational dimension*, referring to the output of such communication, and the *interactional dimension*, referring to the ways in which users interact with these media. The authors use this framework as an entry point to examine specific NN issues that relates to each of these three dimensions: the structural dimension serves as a basis to investigate the issues related to actual access to the Internet infrastructure; the representational dimensions is used as a means to investigate how NN relates to content, with regard to diversity, control, and censorship; and, finally, the interactional dimension is used to describe how new forms of communication that are emerging online could be affected by a derogation to the NN principle. They conclude that NN has become today an important precondition for achieving a properly functioning public sphere, fueled by a variety of information, ideas and opinions.

In addition to promoting freedom of expression, the NN neutrality principle also serves to preserve users' fundamental right to privacy and data protection. Indeed, in order to be able to discriminate amongst packets according to their nature, content, origin or destination, ISPs must rely on sophisticated traffic management techniques – such as Deep Packet Inspection (DPI) – which allows them to examine the content of packets traveling through their . Not only do such intrusive practices risk to jeopardise the open and neutral character of the Internet, but they are also likely to impinge upon the confidentiality of online communications - thereby potentially endangering the privacy of Internet users. In their paper on "Net Neutrality: Ending Network Discrimination in Europe", Raegan MacDonald and Giusy Cannella condemn such practices by claiming that "reasonable" traffic management should be limited to the activities which are strictly necessary for the technical maintenance of the network (*i.e.* minimizing congestion, blocking spam, viruses, and denial of service attacks).

Yet, given the technical challenges that most ISP have to face in order to deliver packets without discrimination of content, ports, protocols, origin, or destination, violations of the NN principle must not be evaluated on an absolute basis, but rather assessed according to their context, their justifications, as well as the impact they might have on human rights. In this regard, Alejandro Pisanty analyses "Network Neutrality under the lens of Risk Management", by providing an important framework to assess the likelihood of NN violations, along with suggestions on how to best deal with such violations.

By ascribing to the end-users the responsibility to establish and manage online communications, the end-to-end principle guarantee an active role to all Internet users, while also reducing the spectrum of interferences potentially limiting their ability to receive and impart information, at the network layer. Such an empowerment of the networks' 'edges' may be seen as one of the most significant galvaniser of freedom of expression in recent history. However, the great success of the Internet had democratised the network and widened its user-base, which is nowadays composed of less technically-erudite users compared to the original community of Internet-pioneers. Indeed, as highlighted by Louis Pouzin in his paper on "Net Neutrality and Quality of Service," a dominant majority of end-users are not (interested in becoming) network experts. This element adds further complexity to the meaning and implementation of the NN principle. In fact, the NN debate is usually based on various assumptions as regards network usage and characteristics. For this reason, the author explores the various standpoints and interpretations of different actor, including network operators, content providers and end-users.

Yet, the rise of cyber-crime and the growing threats to network integrity and security have stimulated the development of "trust-to-trust" models, where private entities (such as ISPs, CAPs or DNS operators) undertake some forms of "network-patrolling" in order to provide a more trustworthy network. It is therefore the democratization of the Internet which spurred the establishment of several form of intermediations to ensure the provision of secure Internet communication - thus transforming the Internet into an increasingly centralized network structure.

Although certain types of network management are essential to guarantee network integrity and security, Internet traffic management (ITM) practices can affect the way in which end-users receive and impart information, thus limiting their capability to freely communicate. For this reason, in his paper on "Net Neutrality: Past Policy, Present Proposals, Future Regulation," Chris Marsden highlights the fact that traffic discrimination can lead of censorship. Therefore, the NN debate can be considered as the latest phase of an eternal argument over control of communications media. Throughout this paper, the author presents the evolution of the NN regulatory debate, providing important elements for a transatlantic comparison. On the one side, U.S. jurisprudence underscores the role of NN regulation in fighting anti-competitive practices, while promoting accessibility and reducing barriers to enter the market. On the other side of the Atlantic, the question of NN cannot be properly analysed within the competition law framework alone, because - as stressed by the author - although the fair competition dimension of net neutrality regulation should not be neglected, it is of utmost importance to properly stress the human rights implication of this crucial debate.

In fact, ISPs' position as "gatekeepers" may allow them to undertake an unchecked and unbalanced role as self-regulators, whose action is not framed by due process and rule of law principles. The regulation of ISPs' traffic management practices is therefore instrumental to avoid dangerously unpredictable agglomerations of power in the hands of ISPs, safeguarding media pluralism and sheltering end-users' fundamental rights.

To this latter extent, in his 'Privatised Online Enforcement Series' Joe McNamee underscores that, although most western democracies are grounded on the "rule of law", they frequently encourage Internet intermediaries' self-regulation in a multitude of domains that have direct implications with regard to the protection of fundamental rights. Indeed, as stressed by the Advocate General of the European Court of Justice, Internet intermediaries' self-regulation equals to "delegating the legal and economic responsibility of the fight against illegal downloading to Internet access providers." These practices are criticized by the author, according to which the proliferation of self-regulatory solutions is based on the arguably questionable assumption that, however distasteful it is that private companies regulate and enforce the law in the online world, "it is better that 'somebody' is doing 'something'"

The existence of numerous discriminatory ITM practices has been highlighted by the Body of European Regulators of Electronic Communications with regard to mobile Internet, and the capability of such techniques to expose Internet users' personal data has been explicitly stressed by the European Data Protection Supervisor. These authoritative opinions suggest the need for an appropriate reflexion on NN, taking into consideration both the fair-competition and the human-rights dimension of the NN debate, with the help of reliable data. Indeed, both Marsden and Pouzin argue that, without factual observation of the service characteristics, there cannot be any credible assertion of NN and the elaboration of evidence-based policy-making becomes simply not possible.

Therefore, it is right and proper to note that the scope of NN regulation is not limited to the definition of this all-important principle and its limits, but rather encompasses the delineation of an appropriate monitoring and enforcement mechanism. A NN regulatory framework is

indeed instrumental to the achievement of three different goals: (i) clarifying what NN is and what is not; (ii) empowering Internet users, by ascribing them the right to undertake an action in front of the relevant authority upon violation of the NN principle; and (iii) investing national regulators with the powers and prerogatives needed in order to establish an appropriate monitoring and enforcement mechanism.

As highlighted by Luca Belli and Matthijs van Bergen, the Dynamic Coalition on Network Neutrality has been created as a self-organised, bottom-up collaborative effort, with the intention of fostering "A Discourse-Principle Approach to Network Neutrality", thus analysing the various nuances of the NN argument and elaborating a model framework through a multi-stakeholder participatory approach. Indeed, it seems obvious that the inherent complexity of the NN debate, as well as the heterogeneity of the stakeholders involved, demand the institution of multi-stakeholder dialogue as an essential pre-condition for the elaboration of policy-recommendation on this delicate matter. The discussion arena provided by the Dynamic Coalition on Network Neutrality aims at generating momentum on this central issue, with the final goal of elaborating a model framework able to provide guidance to national legislators on how to properly safeguard net neutrality.

The following papers explore some of the most crucial facets of NN, underscoring its close relationship with the full enjoyment of end-users fundamental rights. Lastly, this report includes a proposal for a Model Framework on Network Neutrality that has been elaborated by the Dynamic Coalition through an open, inclusive and multi-stakeholder effort, in order to promote an efficient safeguard of the NN principle in accordance with international human rights standards.

References:

BEREC (2012), Overview of BEREC's approach to net neutrality, 27 November 2012, available at http://berec.europa.eu/files/document_register_store/2012/12/BoR_(12)_140_Overview+of+BEREC+approach+to+NN_2012.11.27.pdf

Council of Europe (2011), Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet: https://wcd.coe.int/ViewDoc.jsp?id=1835707.

European Commission (2013), Proposal for a regulation of the European Parliament and of the Council, laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012, COM(2013) 627 final: http://ec.europa.eu/transparency/regdoc/rep/1/2013/EN/1-2013-627-ENF1-1.Pdf.

European Parliament (2012a) Committee on the Internal Market and Consumer Protection, 2012, Report on Completing the Digital Single Market (2012/2030(INI)), A7-034/2012, 26.10.2012, available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//NONSGML+REPORT+A7-2012-0341+0+DOC+PDF+V0//EN

European Parliament (2012a), Report on a Digital Freedom Strategy in EU Foreign Policy (2012/2094(INI), A7-0374/2012, 15.11.2012, available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2012-0374+0+DOC+PDF+V0//EN&language=EN

OECD (2005), Input to the United Nations Working Group on Internet Governance (WGIG), 2005:http://www.oecd.org/sti/ieconomy/ebookoecdinputtotheunitednationsworkinggrouponinternetgovernance.htm#pro

World Bank Group, Summary of the 2009 World Bank Group Report here: http://web.worldbank.org/WBSITE/EXTERNAL/NEWS/0,,contentMDK:22231347~pagePK:34370~piPK:34424~theSitePK:4607,00.html.

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

Network Neutrality and Human Rights
An Input Paper

by Luca Belli

The original version of this paper has been utilised as a Background Paper for the Multi-Stakeholder Dialogue on Network Neutrality and Human Rights[1], a conference organised under the aegis of the Council of Europe on 29-30 May 2013,[2] during which the creation of the Dynamic Coalition on Network Neutrality was proposed by this autor. This paper aims at providing inputs in order to stimulate further reflection pertaining to the relationship between network neutrality and human rights. This paper is obviously not meant to be exhaustive but rather to offer some 'food for thought' in the hope that the instillation of such ideas will trigger constructive discussions.

The origin of the network neutrality concept

The concept of network neutrality (NN) refers to a principle according to which all electronic communication networks shall carry data flows in a non-discriminatory fashion regardless of their nature, their content or the identity of their sender or recipient.

Indeed, NN may be considered as a "network design principle" [3], as a "policy priority"[4] or, rather, as normative principle according to which a maximally useful public information network aspires to treat all content, sites, and platforms equally, thus granting to all Internet users universal access to all online resources.

The debate concerning NN originated at the beginning of the 2000s[5]. The underlying argument in favour of NN is the end-to-end (E2E) principle[6], whereby the intelligence of the network shall be found on its edges, not within the network itself. Indeed, this fundamental principle ascribes to the end-users (which are considered as the "edges" of the network) an

[1] This is a slightly updated version of the original Background Paper. Thanks are due to (in alphabetic order) Kirsten Fiedler, Lee Hibbard, Raegan MacDonald and Frode Sørensen for their very helpful comments on an earlier draft.
[2] The Background Papre was subsequently communicated to the Council of Europe Steering Committee on Media and Information Society (CDMSI). See: http://www.coe.int/t/informationsociety/NN%20Conf%202013/
[3] See: Tim Wu, "Network Neutrality, Broadband Discrimination", in *Journal of Telecommunications and High Technology Law*, Vol. 2, p. 141, 2003.
[4] See: BEREC, Overview of BEREC's approach to net neutrality, 27 November 2012.
[5] See: Mark Lemley and Lawrence Lessig, "The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era" (October 1, 2000) in *UCLA Law Review*, Vol. 48, p. 925, 2001.
[6] 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.

active role consisting in the "responsibility for the integrity of communication"[7], whilst the communications network are considered as a passive and "dumb" infrastructure.

Hence, the NN debate focuses on the relation between the telecommunications operators that manage the various networks composing the Internet and provide Internet access; the Content and Application Providers (CAPs) that offer services, applications and content through the Internet; and end-users. Such debate aims at scrutinising the extent to which network operators – or Internet Service Providers[8] (ISPs) – should be allowed to manage Internet traffic without hindering the full enjoyment of human rights and fundamental freedoms.

Indeed, it should be remarked that certain Internet Traffic Management (ITM) practices, that are not temporary and exceptional, consisting in blocking, filtering, throttling or prioritising specific data flows, have been criticized by several stakeholders, because their utilisation may jeopardise end-users' fundamental rights and compromise the very architecture of the Internet. Such an open and neutral architecture is grounded on the E2E principle and has been essential to the development of the Internet, fostering freedom of expression and innovation, and nurturing media pluralism.

Both the NN principle and the end-to-end argument are grounded on the overarching principle of "openness"[9], which implies universal and reciprocal access amongst all Internet users, fostering freedom of expression as well as the circulation of digital products and services. Indeed, according to NN advocates, the various flows of information running through the different networks should not be blocked or degraded by telecommunications operators, so that end-users can freely impart and receive information and ideas through the network, thus circulating their innovations[10].

[7] According to the Request for Comments n° 1958, "[…] certain required end-to-end functions can only be performed correctly by the end-systems themselves. A specific case is that any network, however carefully designed, will be subject to failures of transmission at some statistically determined rate. The best way to cope with this is to accept it, and give responsibility for the integrity of communication to the end systems". See: Network Working Group, *Request for Comments: 1958, Architectural Principles of the Internet*, June 1996. In addition, according to the Declaration by the Committee of Ministers on Internet governance principles, "[t]he open standards and the interoperability of the Internet as well as its end-to-end nature should be preserved. These principles should guide all stakeholders in their decisions related to Internet governance. There should be no unreasonable barriers to entry for new users or legitimate uses of the Internet, or unnecessary burdens which could affect the potential for innovation in respect of technologies and services". See: Declaration by the Committee of Ministers on Internet governance principles (Adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies), n°8 Architectural principles.

[8] In this paper, the term Internet Service Provider (ISP) refers to any legal person that offers Internet access service to the public or Internet transit service to another ISP.

[9] According to the Declaration by the Committee of Ministers on Internet governance principles, an open network implies that "[u]sers 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. Traffic management measures which have an impact on the enjoyment of fundamental rights and freedoms, in particular the right to freedom of expression and to impart and receive information regardless of frontiers, as well as the right to respect for private life, must meet the requirements of international law on the protection of freedom of expression and access to information, and the right to respect for private life. See: Internet Society, *Open Inter-networking*.

[10] To this latter extent, see: Mark Lemley and Lawrence Lessig (2000); Milton Mueller et al. (2007); Tim Wu (2003).

The NN debate has been fostered by several academics from the United States of America that started questioning the neutral character of the traffic management techniques which are adopted by a number of network operators. To this extent, both Lemley and Lessig (2000) and Wu (2003) developed the claim that such techniques can be deemed as discriminatory. Such an assertion has been corroborated, in 2005, by the notorious Madison River case River case, in which a U.S. telephone company was found guilty of using port blocking to prevent its subscribers from using voice over IP service offered by the ISP Vonage[11].

After having fined Madison River, the U.S. Federal Communications Commission adopted a Policy Statement[12], aimed at promoting the open and neutral nature of the Internet. The FCC Policy Statement represented the first regulatory approach towards NN, establishing four basic rules, according to which internet users are entitled to:

- access the lawful Internet content of their choice;
- run applications and use services of their choice, subject to the needs of law enforcement;
- connect their choice of legal devices that do not harm the network;
- competition among network providers, application and service providers, and content providers.

The NN debate has subsequently gained political momentum and propagated at the European level during the revision of the EU Telecoms Package[13].

The close relationship between the NN principle, freedom of expression and the right to private life has led the Council of Europe's Committee of Ministers to enshrine the NN principle into a specific declaration, according to which "Internet 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"[14].

By virtue of the aforementioned Declaration, the Council of Europe has indeed declared "its commitment to the principle of network neutrality"[15].

Lastly, it has to be stressed that the public debate concerning NN encompasses two dimensions, which are closely related. The first one takes into consideration the opportunity to regulate internet traffic management and to limit network operators' ability to prioritise different data flows. To this extent, it has been argued that the implementation of minimum "quality of service"[16] standards might prove helpful to mitigate certain negative effects of network-management policies, such as the degradation of network performance.

[11] See: Milton Mueller et al., *Neutrality as Global Principle for Internet Governance*, 5 November, 2007, p. 6.
[12] See: Federal Communications Commission, Policy Statement, released: September 23, 2005.
[13] As an instance, see: La Quadrature du Net, Protecting Net Neutrality in the Telecoms Package, September 22 2009.
[14] See: 2010 Declaration of the Committee of Ministers on Network Neutrality, para. 4.
[15] See: 2010 Declaration of the Committee of Ministers on Network Neutrality, para. 9.
[16] According to the Body of European Regulators of Electronic Communications (BEREC), the quality of users' interaction with services is assessed by the Quality of Service (QoS) concept which includes both the network

On the other hand, the second dimension of the NN debate focuses on the universal and reciprocal access to all the resources connected to the internet. As highlighted above, such an approach stems from the end-to-end principle and seeks to prevent the blocking of access to web sites by network operators and the establishment of so-called "walled gardens" limiting access to content, applications and services[17].

This latter dimension conveys the NN debate into the province of human rights and fundamental freedoms, highlighting the possible interferences of anti-NN practices with the enjoyment of freedom of expression. Indeed, as it has been highlighted by the European Data Protection Supervisor, "if this behaviour became common practice and it was not possible (or highly expensive) for users to have access to an open Internet, this would jeopardise access to information and user's ability to send and receive the content they want using the applications or services of their choice"[18].

Reasons and nature of Internet traffic management

It should be noted that, by design, the transmission of data packets through the Internet is organised through the principle of "best effort", according to which ISPs convey internet traffic without any guarantee of quality or obligation over the result.

However, although data-packets are conveyed according to a mere best-effort obligation, a number of specialised CAPs are based on the provision of high-quality access to applications and content. Hence, although Internet access and transit providers convey data with no guarantee of performance, many CAPs heavily rely on quality control in order to provide their services.

The aforementioned Internet services may include IP television (IPTV), video on demand, Voice over IP (VoIP), or Virtual Private Networks (VPN). Because of the wide variety of services and applications that can be delivered over a broadband Internet, carriers are considering "new" business models that differentiate the speed or priority with which packets are delivered. Indeed, prioritisation is usually motivated by a desire to deliver high-quality video content or services, which require continuous streaming and consume a considerable amount of bandwidth.

To this latter extent, many telecommunications carriers have adopted network management policies and implemented "packet prioritisation" capabilities that can improve the quality of

---

and the terminal equipment. The strict technical term QoS includes many parameters outside the control of the network provider

Therefore, for technical purposes the Network Performance concept is used for measurement of the performance of network portions that are under individual providers' control. Measuring the performance of individual traffic flows originating from specific applications may be a necessary part of any test configuration for detection of blocking and throttling of applications. See: BEREC, *A framework for Quality of Service in the scope of Net Neutrality*, 8 December 2011, pp. 3-4.

[17] See: Milton Mueller *et al.*, *Neutrality as Global Principle for Internet Governance*, 5 November, 2007.

[18] See: *Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data*, 7 October 2011, p. 4.

specific Internet services, by prioritising specific data flows. However, as it has been revealed by the Madison River case, traffic-management practices may jeopardise the open and neutral character of the Internet, and data prioritisation may lead to discriminatory and abusive practices[19].

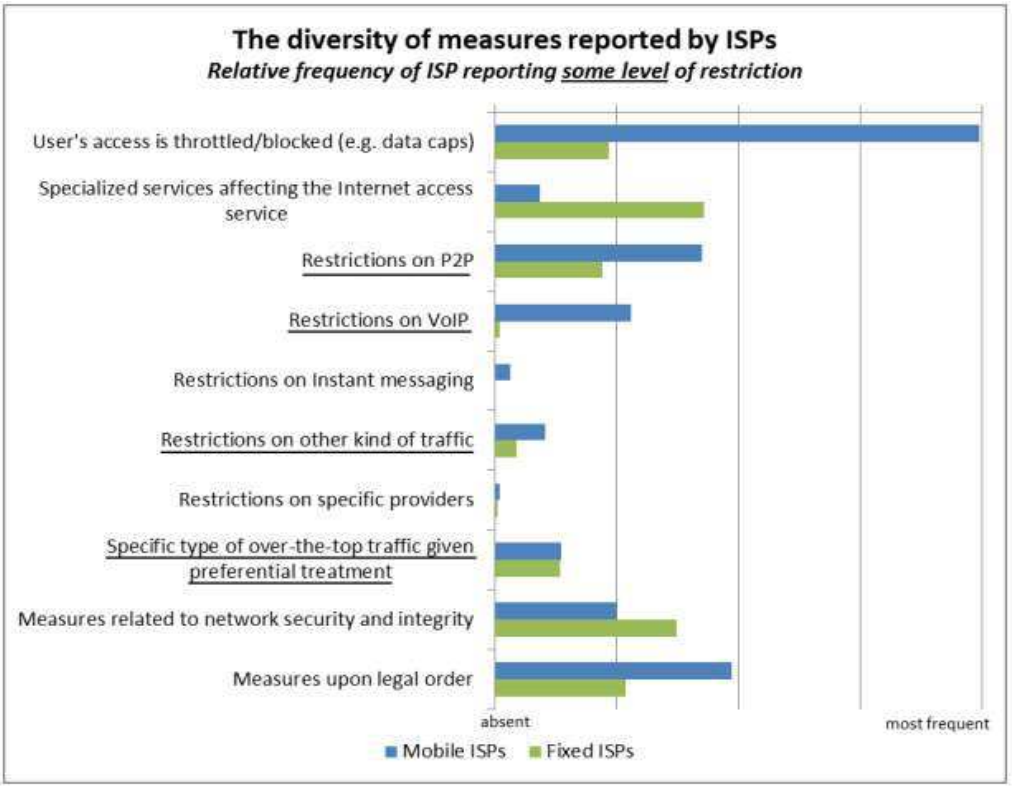
At the EU level, a joint investigation of the Body of European Regulators of Electronic Communications (BEREC) and the European Commission has recently highlighted the existence of a wide array of traffic management practices resulting in restrictions, and has scrutinised the corresponding implementation methods and policy justifications[20].

Indeed, there is growing fret that telecoms operators and ISPs, are exploiting network management techniques to favour their commercial partners or the services and applications with which they vertically integrate[21]. In fact, the existing "differentiation" practices may result in restrictions to access specific content or applications such as VoIP, Peer-to-Peer protocols (P2P) or other specific providers.

Particularly, four categories of network management practices have been documented at European level:

- Throttling bandwidth-intensive protocols. In this case, Internet access and transit providers throttle specific class of Internet traffic in order to lower their infrastructure costs. As an instance, peer-to-peer traffic has been frequently subject to such discriminatory practices whereby network operators prioritise traffic to ensure that specific protocols will enjoy better quality of service;
- Inhibiting competing services. Such practice consists in blocking specific protocols or applications and might be adopted to weaken potential competitors. To this extent, network operators may inhibit protocols allowing competing services – such as VoIP – or charge extra fees for their use, in order to preserve their business model;
- Potential Internet "tolls". Such practice consists in imposing specific fees to service providers in order to enjoy various levels of quality of service. Although such practice has not been put in place yet, it is increasingly contemplated by several ISPs[22];
- Blocking access to content, applications and services on the request of national governments.

[19] See: La Quadrature du Net, Time for EU-Wide Net Neutrality Regulation, Response to the European Commission's questionnaire on Net neutrality, September 30th, 2010, pp. 3-4.
[20] In the conclusions of its Communication on the open internet and net neutrality in Europe issued on the 19th of April 20112, the Commission indicated that the evidence found by BEREC would serve as a basis for assessing the potential need for additional guidance on net neutrality. See: BEREC, *A view of traffic management and other practices resulting in restrictions to the open Internet in Europe*, Findings from BEREC's and the European Commission's joint investigation, 29 May 2012.
[21] See: BEREC, Draft Report Assessment of IP-interconnection in the context of net neutrality, 6 December 2012.
[22] See: *Idem.*



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

Although some traffic-management techniques may be applied sporadically and for a limited period of time, the breath of such phenomenon holds promise to interfere with the internet users' right to receive and impart information and ideas. Notably, interferences may be particularly evident with regard to mobile internet access, where several management techniques are commonly put in place, targeting specific services, applications or protocols.

Network management may lead to human rights violations

As it has been highlighted above, traffic management techniques are currently widespread and may be utilised for a number of different purposes. Moreover, in order to put in place Internet traffic management, network operators may exploit intrusive technical means.

On the one hand, network-management techniques may give rise to thorny phenomena such as over-blocking, filtering and throttling as well as invasive packet inspection. On the other hand, it should be noted that ISPs' gate-keeper position allows these entities to implement various forms of self-regulation that are not framed by due-process and rule-of law principles and that may turn into privatised censorship.

Network operators might be tempted to use Deep Packet Inspection (DPI) technologies and the like in order to identify the content and applications which they intend to block, prioritise or downgrade. Indeed, such technologies are currently available for both fixed and wireless

networks, and they may be exploited to monitor networks for many purposes, amongst which the prevention of online pornography and copyright infringement[23]. In the UK, for example, DPI technology Clean Feed has already been imposed on internet access providers to block access to child abuse material and alleged copyright infringements[24].

By all means, the adoption of such invasive techniques may have nefarious consequences on Internet users' fundamental right to private life, which is guaranteed by a number of international human rights standards. Particularly, it seems difficult to reconcile DPI techniques with the protection of the privacy of communications granted by Article 8 of the European Convention on Human Rights, and with Internet users' data privacy, explicitly sheltered by the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and further elaborated by Recommendation N° R (99) 5 of the Committee of Ministers to member states on the protection of privacy on the Internet.

Hence, it is of utmost importance to be aware that the illegitimate, disproportional and unnecessary[25] use of "application-specific"[26] ITM measures may endanger Internet users' freedom of communication, with particular regard to their right to impart and receive information, and may put in jeopardy the Internet users' right to private life. Furthermore, such techniques have the potential to seriously affect media pluralism and to hinder the circulation of end-users' innovations.

To this extent, several states have enshrined NN in their national legal systems and some observers suggest that a legally mandatory principle of NN may be meaningful in order to guarantee both competition and the full enjoyment of human rights[27].

A human-rights-oriented approach

As highlighted above, an access-oriented approach to NN focuses on preserving the universal, reciprocal and non-discriminatory access to any lawful content, services or application on the Internet, and the reciprocal right to have their resources universally accessible to other internet users.

However, it should be stressed that blocking access to Internet resources, as well as traffic filtering,[28] may be mandated by law in order to prevent specific behaviours. Indeed, some

[23] See: Milton Mueller *et al.*, *Neutrality as Global Principle for Internet Governance*, *op. cit.*
[24] See: UNESCO, *Liberté de connexion Liberté d'expression - Ecologie dynamique des lois et règlements qui façonnent l'Internet*, 2012.
[25] These criteria have been elucidated by the jurisprudence of the European Court of Human Rights in order to delineate "margin of appreciation" of Council of Europe members with regard to the application of the ECHR. The term "margin of appreciation" is a common notion in administrative law systems and the ECtHR utilises it to refer to the space for manoeuvre granted to national authorities, in fulfilling their obligations under the ECHR.
[26] The term application-specific refers to those ITM techniques that target specific content, applications or uses.
[27] As an instance, see: Conseil National du Numérique, Rapport relatif à l'avis « Net Neutralité » n°2013-1 du 1er mars 2013.
[28] It should be stressed that the expression "blocking" refers to the prevention of a communication without inspecting content, whereas the expression "filtering" implies that the content be inspected before being blocked. Notably, those techniques may consist in: (i) blocking an IP address: in this case ISPs block packets with an

national legislators impose blocking and filtering techniques in order achieve various policy goals, despite growing awareness that such techniques are not efficient, costly and can be easily circumvented[29]. To this latter extent, national legislators can design blocking and filtering measures, as long as those techniques respond to a legitimate objective.

Nevertheless, it seems essential that, in order to prevent violations of the European Convention on Human Rights, blocking and filtering be utilised exclusively to fulfil pressing-social-needs and be strictly defined by a precise legal or regulatory framework.

Furthermore, traffic management techniques should be considered as deviations from the NN principle to which the Council of Europe has explicitly committed[30] and, therefore, they should be allowed only temporarily and under specific circumstances, justified either on grounds of verifiable technical necessity or to address a transient network management problem which cannot otherwise be addressed[31].

address in their header that is listed as an IP address to be blocked directly at the router level or distribute "wrong paths" thus attracting packets destined to addresses that are included on a list of blocked IP addresses; (ii) blocking a domain name: in this case, ISPs falsify the responses to DNS queries by not providing the IP addresses that correspond to blocked domain name; (iii) filtering by content inspection: this technique requires installing content inspection servers so that the entirety of the traffic passes through these servers. The servers then allow the content of the packets to be analysed and blocked according to a wide range of criteria; (iv) blocking URLs: this method combines blocking and filtering and aims at blocking requests by URLs listed as blocked.

[29] See: European Commission, *Staff working document on Online Gambling*, 2012, p. 62.

[30] See: 2010 Declaration of the Committee of Ministers on Network Neutrality, op. cit., para. 9

[31] See: The European Consumer Organisation and European Digital Rights, *Call for Action: Time to truly protect Net Neutrality in Europe*, April 2013.

ANNEXE 1:
Council of Europe – Declaration of the Committee of Ministers on Network Neutrality

[…] 4. 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. Such a general principle, commonly referred to as network neutrality, should apply irrespective of the infrastructure or the network used for Internet connectivity. Access to infrastructure is a prerequisite for the realisation of this objective.

5. There is an exponential increase in Internet traffic due to the growing number of users and new applications, content and services that take up more bandwidth than ever before. The connectivity of existing types of devices is broadened as regards networks and infrastructure, and new types of devices are connected. In this context, operators of electronic communication networks may have to manage Internet traffic. This management may relate to quality of service, the development of new services, network stability and resilience or combating cybercrime.

6. In so far as it is necessary in the context described above, traffic management should not be seen as a departure from the principle of network neutrality. However, exceptions to this principle should be considered with great circumspection and need to be justified by overriding public interests. In this context, member states should pay due attention to the provisions of Article 10 of the European Convention on Human Rights and the related case law of the European Court of Human Rights. Member states may also find it useful to refer to the guidelines of Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters.

7. Reference might also be made in this context to the European Union regulatory framework on electronic communications whereby national regulatory authorities are tasked with promoting users' ability to access and distribute information and to run applications and services of their choice.

8. Users and service, application or content providers should be able to gauge the impact of network management measures on the enjoyment of fundamental rights and freedoms, in particular the rights to freedom of expression and to impart or receive information regardless of frontiers, as well as the right to respect for private life. Those measures should be proportionate, appropriate and avoid unjustified discrimination; they should be subject to periodic review and not be maintained longer than strictly necessary. Users and service providers should be adequately informed about any network management measures that affect in a significant way access to content, applications or services. As regards procedural safeguards, there should be adequate avenues, respectful of rule of law requirements, to challenge network management decisions and, where appropriate, there should be adequate avenues to seek redress.

9. The Committee of Ministers declares its commitment to the principle of network neutrality and underlines that any exceptions to this principle should comply with the requirements set out above. This subject should be explored further within a Council of Europe framework with a view to 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.

ANNEXE 2:
National legislation on Network Neutrality

Norwegian principles

1. Internet users are entitled to an Internet connection with a predefined capacity and quality.

2. Internet users are entitled to an Internet connection that enables them to (i) send and receive content of their choice; (ii) use services and run applications of their choice; (iii) connect hardware and use software of their choice that do not harm the network.

3. Internet users are entitled to an Internet connection that is free of discrimination with regard to type of application, service or content or based on sender or receiver address.

Principle 1 states that the characteristics of the Internet connection are to be contracted in advance, also with a view to cases where Internet access is provided together with other services on the same physical connection. Principle 2 states qualitatively that the Internet connection must be able to be used as the user wants. And Principle 3 states that traffic over the Internet connection is to be transferred in a non-discriminatory manner[32].

Dutch legislation

Article 7.4a, Telecommunications Act (unofficial translation[33])

1. Providers of public electronic communication networks which deliver internet access services and providers of internet access services do not hinder or slow down applications and services on the internet, unless and to the extent that the measure in question with which applications or services are being hindered or slowed down is necessary:

[32] See: Norwegian Post and Telecommunications Authority, *Network neutrality Guidelines for Internet neutrality*, Version 1.0, 24 February 2009, available http://www.legi-internet.ro/fileadmin/editor_folder/pdf/Guidelines_for_network_neutrality_-_Norway.pdf

[33] See: Daphne van der Kroft, "Net Neutrality in the Netherlands: State of Play", in *Bits of Freedom*, 15 June 2011, available at https://www.bof.nl/2011/06/15/net-neutrality-in-the-netherlands-state-of-play/

a) to minimize the effects of congestion, whereby equal types of traffic should be treated equally;
b) to preserve the integrity and security of the network and service of the provider in question or the terminal of the end-user;
c) to restrict the transmission to an end-user of unsolicited communication as referred to in Article 11.7, first paragraph, provided that the end-user has given its prior consent;
d) to give effect to a legislative provision or court order.

2. If an infraction on the integrity or security of the network or the service or the terminal of an end-user, referred to in the first paragraph sub b, is being caused by traffic coming from the terminal of an end-user, the provider, prior to the taking of the measure which hinders or slows down the traffic, notifies the end-user in question, in order to allow the end-user to terminate the infraction. Where this, as a result of the required urgency, is not possible prior to the taking of the measure, the provider provides a notification of the measure as soon as possible. Where this concerns an end-user of a different provider, the first sentence does not apply.

3. Providers of internet access services do not make the price of the rates for internet access services dependent on the services and applications which are offered or used via these services.

4. Further regulations with regard to the provisions in the first to the third paragraph may be provided by way of an administrative order. A draft order provided under this paragraph will not be adopted before it is submitted to both chambers of the Parliament.

5. In order to prevent the degradation of service and the hindering or slowing down of traffic over public electronic communication networks, minimum requirements regarding the quality of service of public electronic communication services may be imposed on undertakings providing public communica-tions networks.

Slovenian legislation

Article 203rd, Electronic Communications Act (unofficial translation[34])

(1) The Agency encourages the preservation of the open and neutral character of the internet and the access to and dissemination of information or the use of applications and services of their choice of end users.

[34] see: Innocenzo Genna, "Slovenia reinforces net neutrality principles", in *Radiobruxelleslibera*, 3 January 2013, available at http://radiobruxelleslibera.wordpress.com/2013/01/03/slovenia-reinforces-net-neutrality-principles/ ; Slovenian Electronic Communications Act, available at http://www.uradni-list.si/_pdf/2012/Ur/u2012109.pdf#!/u2012109-pdf

(2) The Agency goals in the previous paragraph must be carefully considered in the exercise of its jurisdiction under Articles 3 and 4 the second paragraph of the 132nd of this Act, and the third and fourth paragraphs of the 133rd of this Act and their responsibilities in relation to the implementation of the second of the first paragraph of Article 129 Article by the network operator and provider of Internet access services.

(3) Network operators and Internet access providers shall make every effort to preserve the open and neutral character of the internet, thus it may not restrict, delay or slowing Internet traffic at the level of individual services or applications, or implement measures for their evaluation, except in case:

1. necessary technical measures to ensure the smooth operation of networks and services (e.g., to avoid traffic congestion);
2. necessary steps to preserve the integrity and security of networks and services (e.g., elimination of unfair seizure of over a transmission medium - channel);
3. emergency measures for limiting unsolicited communications in accordance with the 158th of this Act;
4. decision of the court.

(4) The measures provided for in Articles 1, 2 and 3 of the preceding paragraph shall be proportionate, non-discriminatory, limited in time and to the extent that this is necessary.

(5) Network operators' and Internet service providers' services shall not be based on services or applications, which are provided or used by internet access services.

(6) The Agency may implement the provisions of the third, fourth and fifth paragraphs of this Article can issue a general act.

References:

La Quadrature du Net, *Time for EU-Wide Net Neutrality Regulation, Response to the European Commission's questionnaire on Net neutrality*, 30 September 2010, available at http://www.laquadrature.net/files/LQDN-20100930-ReponseNetNeutralityQuestionnaire.pdf

Mark Lemley and Lawrence Lessig, "The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era" (October 1, 2000) in *UCLA Law Review*, Vol. 48, p. 925, 2001, available at: http://ssrn.com/abstract=247737

Christopher T. Marsden, *Net Neutrality: Towards a Co-regulatory Solution*, 2010, available at http://www.bloomsburyacademic.com/view/NetNeutrality_9781849662192/book-ba-9781849662192.xml

Center for Democracy & Technology, *Preserving the Essential Internet*, June 2006, available at https://www.cdt.org/speech/20060620neutrality.pdf

The European Consumer Organisation and European Digital Rights, *Call for Action: Time to truly protect Net Neutrality in Europe*, April 2013, available at http://edri.org/files/2013-BEUC-EDRi-NN.pdf

Milton Mueller *et al.*, *Neutrality as Global Principle for Internet Governance*, 5 November, 2007, available at http://www.internetgovernance.org/wordpress/wp-content/uploads/NetNeutralityGlobalPrinciple.pdf

Internet Society, *Open Inter-networking*, 21 February 2010, available at http://www.internetsociety.org/sites/default/files/Open%20Inter-networking%20Getting%20the%20fundamentals%20right-%20access,%20choice,%20and%20transparency.pdf

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, available at http://web.mit.edu/saltzer/www/publications/endtoend/endtoend.pdf

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

UNESCO, Liberté de connexion Liberté d'expression - Ecologie dynamique des lois et règlements qui façonnent l'Internet, 2012, available at http://unesdoc.unesco.org/images/0021/002160/216029f.pdf

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

CoE sources:

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

Committee of Ministers Declaration on Internet Governance Principles, available at https://wcd.coe.int/ViewDoc.jsp?id=1835773&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

Recommendation CM/Rec(2008)6 of the Committee of Ministers on measures to promote the respect for freedom of expression and information with regard to Internet filters, available at https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282008%296&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75

2003 Declaration of the Committee of Ministers on freedom of communication on the Internet, available at http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Dec%282003%29FreedomCommInt_en.asp#TopOfPage

Recommendation CM/Rec(2010)13 of the Committee of Ministers on the protection of individuals with regard to automatic processing of personal data in the context of profiling, available at https://wcd.coe.int/ViewDoc.jsp?id=1710949&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

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

Human rights guidelines for Internet service providers Developed by the Council of Europe in co-operation with the European Internet Services Providers Association (EuroISPA), available at http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf%282008%29009_en.pdf

EU sources and documents:

BEREC, A framework for Quality of Service in the scope of Net Neutrality, 8 December 2011, available at http://berec.europa.eu/doc/berec/bor/bor11_53_qualityservice.pdf

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

BEREC, Draft Report Assessment of IP-interconnection in the context of net neutrality, 6 December 2012, available at http://berec.europa.eu/eng/document_register/subject_matter/berec/public_consultations/?doc=33

BEREC, Guidelines on Net Neutrality and Transparency: Best practices and recommended approaches, available at http://berec.europa.eu/files/news/consultation_draft_guidelines.pdf

BEREC, Overview of BEREC's approach to net neutrality, 27 November 2012, available at http://berec.europa.eu/files/document_register_store/2012/12/BoR_(12)_140_Overview+of+BEREC+approach+to+NN_2012.11.27.pdf

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF

EDPS, Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data, 7 October 2011, available at http://ec.europa.eu/bepa/european-group-ethics/docs/activities/peter_hustinx_presentation_(1)_15_rt_2011.pdf

European Commicssion, The Open Internet and Net Neutrality in Europe, Communication from the Commission to the European Parliament, the Council the Economic and Social Committee and the Committee of the Regions, Brussels, 19.4.2011, COM(2011) 222 final, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0222:FIN:EN:PDF

European Commission, Staff working document on Online Gambling, 2012, p. 62, available at http://ec.europa.eu/internal_market/gambling/docs/121023_online-gambling-staff-working-paper_en.pdf

The open internet and net neutrality in Europe, European Parliament resolution of 17 November 2011 on the open internet and net neutrality in Europe, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2011-0511+0+DOC+PDF+V0//EN

European Commission, *Staff working document on Online Gambling*, 2012, available at http://ec.europa.eu/internal_market/gambling/docs/121023_online-gambling-staff-working-paper_en.pdf

National reports

Autorité de régulation des communications électroniques et des postes, Report to Parliament and the Government on Net Neutrality, September 2012, available at http://www.arcep.fr/uploads/tx_gspublication/rapport-parlement-net-neutrality-sept2012-ENG.pdf

Conseil National du Numérique, Rapport relatif à l'avis « Net Neutralité » n°2013-1 du 1er mars 2013, available at http://www.cnnumerique.fr/wp-content/uploads/2013/03/130311-rapport-net-neutralite-VFINALE.pdf

French National Assembly, Report on Net and Network Neutrality, April 13, 2011, available at http://www.assemblee-nationale.fr/english/dossiers/net_and_network_neutrality.pdf

Norwegian Post and Telecommunications Authority, Network neutrality Guidelines for Internet neutrality, Version 1.0, 24 February 2009, available http://www.legi-internet.ro/fileadmin/editor_folder/pdf/Guidelines_for_network_neutrality_-_Norway.pdf

The Importance of Internet Neutrality to Protecting Human Rights Online

by Andrew McDiarmid and Matthew Shears

Introduction

The history of the Internet has shown that it has tremendous capacity to advance human rights, in particular freedom of expression and related rights. Over 2 billion people around the world connect every day to access and share information and participate in wide-ranging aspects of social, economic, and political life. For individuals, connecting to the Internet provides access to an ever-expanding array of information resources and online services. At the same time, it offers opportunities for people to reach new audiences at very low cost compared to other forms of mass media. To an unprecedented degree, the Internet transcends national borders and reduces barriers to the free flow of information, enabling free expression, democratic participation, and the enjoyment of other rights.

At least, it can. Merely having Internet access is not sufficient to guarantee the full flowering of free expression and the other rights it enables, including the rights to freedom of assembly and association, the right to education, and the right to participate in cultural life. The Internet's power to transform communications and promote free expression and a pluralistic information environment flows from certain characteristics that have defined the Internet since its inception. These characteristics are not immutable, however, and are increasingly subject to pressure. To maximize the Internet's potential to advance human rights, the Internet must remain free from centralized controls, open to the fullest range of content and services, and truly global. Establishing rules to preserve net neutrality – or more precisely, Internet neutrality – is one way to prevent the imposition, by those in a position to control access, of structural inequalities that would distort this environment.[1]

Much writing and advocacy related to the Internet and free expression is concerned with state censorship and other curtailment of rights by governments. This is a critically important aspect of online free-expression advocacy, made ever more so by the ongoing revelation, as of this writing, of widespread surveillance of Internet traffic. But governments' duty to protect human rights extends beyond non-interference, particularly in the realm of communications and free expression.[2] And as the telecom sector is increasingly liberalized, private Internet access providers are in a position to control their customers' access to Internet content, often for purely commercial reasons. Discriminatory treatment of Internet traffic by access providers threatens Internet users' ability to seek, receive, and impart information of their own

[1] CDT uses the term "Internet neutrality" to make it clear that neutrality principles should apply only to Internet access, not to non-Internet services offered over broadband infrastructure. We do not argue that neutrality obligations should apply to over-the-top services offered via the Internet.
[2] See infra note 25 and accompanying text.

choosing, and the ability of entrepreneurs around the world to launch new communications tools and services that in turn can advance human rights. Fully protecting user choice and free expression and other rights online therefore requires that governments take steps to prevent access providers from taking actions that may interfere with users' enjoyment of those rights.

CDT's previous work has examined the need for rules to protect neutrality as the Internet evolves.[3] This paper seeks to frame the issue more directly in terms of Internet neutrality's role in fostering a range of human rights, including free expression, access to knowledge, and democratic participation. We also offer a set of principles to guide the enactment of rules to protect Internet neutrality.

Designed for Free Expression

In terms of its technical transmission architecture, the Internet has historically been indifferent to the content transmitted across it. Two fundamental design principles underlie this architecture: layering and the end-to-end principle. Layering creates a logical separation between network functions (such as the addressing and routing of information) and endpoint functions (such as the processing and presentation of content by servers, PCs, and smartphones). The end-to-end principle requires that networks take on only network responsibilities, leaving all other functionality to the endpoints.[4] By analogy to the postal system, endpoints are like people writing and reading letters, while the primary function of ISPs' routers and switches is to read addresses and move information to its destination like the postal service. The result is a general-purpose network than accepts an ever-expanding array of content and applications – ranging from Skype to 'cloud' storage to personal websites. Within the Internet, networks receive and forward communications, without having to make an assessment of what the traffic is (e.g., whether it is an e-mail, a website, or a voice-over-IP call).

This approach permits the greatest level of flexibility for new uses of the Internet, making the Internet an unprecedented platform for free expression and innovation in communications. End users post any content and can invent wholly new applications and services without any changes to the underlying network. It enables any two Internet users – individuals, companies, websites, etc. – to communicate with each other without any need to get permission or make prior arrangements (other than purchasing basic access to the Internet) with their network providers or any other entity in between the two end points.[5] "The Internet is a general purpose technology that creates value not through its own existence, but by enabling users to

[3] See, e.g., CDT, Preserving the Essential Internet, 2006, https://www.cdt.org/paper/preserving-essential-internet..

[4] See J.H. Saltzer, D.P. Reed and D.D. Clark, End-to-End Arguments in System Design, ACM Transactions in Computer Systems 2, 4 November 1984, pp 277-288, http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf.; *see also* Brief of Internet Engineers, *FCC v. Verizon* (US Court of Appeals for the DC Circuit, 11-1355), http://www.fcc.gov/document/internet-engineers-amicus-brief-no-11-1355-dc-cir (a legal brief explaining the technical functionality of the Internet presented to the court considering a legal challenge to the US Federal Communications Commission's rules to establish Internet neutrality).

[5] See Barbara van Schewick, *Internet Architecture and Innovation*, MIT Press, 2010, 72–75, 286–289 (discussing "end-to-end," "application-blind" network architecture).

do what they want. The Internet thus creates maximum value when users remain free to choose the applications they most highly value."[6]

This design has resulted in specific characteristics that support the Internet's power to promote free expression, access to knowledge, and democratic participation through ever-expanding means and opportunities for communication.[7] These defining attributes of the Internet include:

- **Global:** Absent interference, the Internet provides immediate access to information from around the world. For a user, it is as easy to send information to, or receive information from, a user on another continent as it is to communicate with a user in the building next door.
- **User-Controlled:** The Internet allows users to exercise far more choice than even cable/satellite television or short wave radio. As the Internet exists now, a user can skip from site to site in ways that are not dictated by either the content providers or the access provider. User-controlled filtering tools can help users prevent unwanted content from reaching their computers.[8]
- **Decentralized:** The Internet is based on open technical standards and was designed to be decentralized. At the edges of the network, innovators can create a very wide range of applications and offer them without seeking approval or coordination of the entities operating the core of the network. This has meant that, compared to other forms of mass media, the Internet lacks the kind of gatekeepers that exist in legacy print or broadcasting media and offers low barriers to access.
- **Open & Competitive:** The Internet is relatively unconstrained by scarce resources (as compared to, for example, radio and television broadcast channels) and can accommodate an essentially unlimited number of endpoints and speakers. Relative to mass media, there is much greater parity between large and small speakers online. Differences in resources notwithstanding, any individual can post content and make it accessible to the same global audience as that of large media companies.

While these characteristics have historically represented the status quo, access providers are increasingly technologically capable and economically motivated to act in ways that would alter these characteristics to the detriment of individuals' enjoyment of human rights. Internet neutrality is primarily concerned with preserving these characteristics, especially openness.

CDT defines Internet neutrality as the principle that providers of Internet access should not discriminate in their carriage of Internet traffic on the basis of its source, destination, content,

[6] Engineers' brief, *supra* note 4.
[7] *See* CDT, *Regardless of Frontiers: The International Right to Freedom of Expression in the Digital Age*, April 2011, http://www.cdt.org/files/pdfs/CDT-Regardless_of_Frontiers_v0.5.pdf.
[8] See John B. Morris, Jr. & Cynthia M. Wong, "Revisiting User Control: The Emergence and Success of a First Amendment Theory for the Internet Age," U. of N. Carolina First Amendment Law Review, vol. 8, Fall 2009, http://www.cdt.org/files/pdfs/morris_wong_user_control.pdf.

or associated application.[9] Internet neutrality requirements are a key tool for addressing the risk that access providers will distort competition and reduce opportunities for free expression online (for example by slowing the traffic from services that compete with their own offerings). They are critical for ensuring that the Internet continues to promote openness, innovation, and human rights as the role the Internet plays in world economies, governance, and public discourse grows ever larger.

The Internet and Human Rights

The Internet reflects and has substantially advanced two central, forward-looking concepts of international free expression standards: borderlessness and choice. The Universal Declaration of Human Rights states, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas *through any media and regardless of frontiers*."[10] Similarly, Article 19.2 of the International Covenant on Civil and Political Rights states, "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, *regardless of frontiers*, either orally, in writing or in print, in the form of art, or *through any other media of his choice*."

As a decentralized global network, the Internet offers individuals unprecedented power to seek and impart information across borders. It offers not only unprecedented global reach for individual speakers, but also unprecedented capacity for diverse information sources ranging from professional media sites to social networking sites, educational resources such as MIT Open Courseware,[11] and video platforms for audiences to choose from.

Accordingly, there is growing international consensus that the right to freedom of expression must be fully protected on the Internet. In 2011, UN Special Rapporteur for Freedom of Opinion and Expression Frank LaRue issued a landmark report on online free expression, calling the Internet "one of the most important vehicles by which individuals exercise their right to freedom of opinion and expression."[12] LaRue and the special rapporteurs on freedom of expression to regional human-rights bodies for Africa, the Americas, and Europe also jointly issued a set of principles for online free expression, including that "Freedom of expression applies to the Internet, as it does to all means of communication. Restrictions on freedom of expression on the Internet are only acceptable if they comply with established international standards."[13] The Human Rights Committee's ICCPR General Comment 34

[9] Appropriate exceptions should be made for reasonable network management. CDT has written extensively on the practicalities of implementing Internet neutrality rules. *See generally* https://wwwcdt.org/issue/internet-neutrality.
[10] Article 19 (emphasis added).
[11] http://ocw.mit.edu.
[12] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, May 2011, http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/17/27&Lang=E.
[13] Frank LaRue, Dunja Mijatoviæ (Organization for Security and Co-operation in Europe), Catalina Botero Marino (Organization of American States), and Faith Pansy Tlakula (African Commission on Human and Peoples' Rights), Special Rapporteurs' Joint Declaration on Freedom of Expression and the Internet, June 2011, http://www.oas.org/en/iachr/expression/showarticle.asp?artID=848&lID=1.

specifies that protected means of expression "include all forms of audio-visual as well as electronic and internet-based modes of expression."[14] And in 2012 the Human Rights Council issued a resolution that the "same rights that people have offline must also be protected online, in particular freedom of expression."[15]

Moreover, free expression is an enabling right, the exercise of which feeds directly into the exercise of other social, cultural, economic and political rights, "such as the right to education[,] . . . the right to take part in cultural life and to enjoy the benefits of scientific progress and its applications, . . . [and] the rights to freedom of association and assembly."[16] And experience has shown how the Internet can empower not just individual free expression and access to information, but also political discourse, participation in culture, and economic development.[17] This magnifies the Internet's unique power to advance a range of human rights and underscores the importance of preserving that power through meaningful Internet neutrality rules.

Internet Neutrality's Role in Fostering Human Rights

In human-rights terms, preserving Internet neutrality means preserving the power of individuals to make choices about how they use the Internet – what information to seek, receive, and impart, from which sources, and through which services. This in turn advances the other cultural and civil and political rights listed in the previous section.[18]

Violations of the neutrality principle that amount to blocking certain information resources or restricting what information Internet users can impart over their connection would have serious implications for the right to free expression. For example, blocking access to a particular lawful blog because its content is disfavored by the access provider would raise obvious concerns. Indeed, the blocking of Internet content by states has long been a leading concern of Internet–free expression advocates and was a major focus of the UN Special Rapporteur's report.[19]

---

[14] UN Human Rights Committee, General Comment 34, ¶ 12.
[15] Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/20/8, 17 June 2012, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8.
[16] UN Special Rapporteur's Report, *supra* note 12.
[17] *See* CDT, *Regardless of Frontiers*, *supra* note 7; *see also* McKinsey, *Online and upcoming: The Internet's impact on aspiring countries*, January 2012, http://www.mckinsey.com/client_service/high_tech/latest_thinking/impact_of_the_internet_on_aspiring_countries.
[18] *See, e.g.*, Human Right Council, Report of the Special Rapporteur on the rights of peaceful assemble and association, Maina Kiai, May 2012, ¶ 32, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A-HRC-20-27_en.pdf. ("The Special Rapporteur notes the increased use of the Internet, in particular social media, and other information and communication technology, as basic tools which enable individuals to organize peaceful assemblies.")
[19] *See supra* note 12, ¶ 31 ("States' use of blocking or filtering technologies is frequently in violation of their obligation to guarantee the right to freedom of expression." In addition, the report concludes that "while States are the duty-bearers for human rights, private actors and business enterprises also have a responsibility to respect human rights").

In the Internet neutrality context, however, outright blocking often poses a much less realistic threat than the risk that access providers will seek to discriminate among different types or providers of Internet content. Discrimination among content can refer to either prioritizing or slowing down certain content for delivery over an access provider's network. When the net neutrality debate first flared in the US in the mid 2000s, broadband company executives made statements not about blocking per se, but about their desire either to obtain payment from the services their subscribers used or to enter into special arrangements with certain content providers to guarantee faster delivery speeds. This desire – to be paid by content providers for carrying their traffic – has continued to manifest in disputes over the terms by which large content networks (such as Google/YouTube) and large access providers (such as France Telecom–Orange) interconnect and exchange traffic.[20] And there appears to be a growing trend toward "sponsored data" arrangements, particularly in the mobile market, under which content providers make deals with access providers to exempt their content and services from data usage caps.[21]

Discriminatory treatment of traffic has a more subtle but nonetheless meaningful impact on users' rights. First, the means of identifying traffic to carry out discriminatory treatment may impact the privacy of users' communications. In addition, choosing freely from among the myriad content, applications, and services available on the open Internet is an important part of the exercise of the right to free expression online. If access providers speed up or slow down access to certain sites, that choice risks becoming the illusion of choice, with users unwittingly steered toward particular content or services they might not have otherwise chosen.

Moreover, the Internet is not simply another mass medium for the one-way dissemination of content and information; it is also a platform for the development of new communications tools. Much like the way the free expression right is an enabler of other rights, the Internet is an enabler of varied, diverse media and services that in turn advance the enjoyment of free expression and other rights. Internet neutrality helps preserve a competitive market for such online content and services, fostering a diverse array of information sources and communication tools that enables the enjoyment of human rights by users of those tools. New competitors benefit tremendously from the open Internet's low barriers to entry. Once a

[20] *See* Ewan Spence, "Why Orange's Dominance in Africa Forced Google To Pay For Traffic Over The Mobile Network", *Forbes*, 20 January 2013, http://www.forbes.com/sites/ewanspence/2013/01/20/why-oranges-dominance-in-africa-forced-google-to-pay-for-traffic-over-their-mobile-network/. Providers of Internet access have been roundly criticized for regulatory proposals to favor payment from content and application providers for the delivery of their traffic to Internet users. *See* Body of European Regulators for Electronic Communications, BEREC's comments on the ETNO proposal for ITU/WCIT or similar initiatives along these lines, November 2012, http://berec.europa.eu/eng/document_register/subject_matter/berec/others/1076-berecs-comments-on-the-etno-proposal-for-ituwcit-or-similar-initiatives-along-these-lines; CDT, *ETNO Proposal Threatens Access to Open, Global Internet*, June 2012, https://www.cdt.org/report/etno-proposal-threatens-access-open-global-internet.

[21] Data usage caps are numerical limits on the amount of data a subscriber to an Internet access provider may use per month. See e.g., Bruce Houghton, "Spotify Adds Germany's Deutsche Telekom To Growing List Of Mobile Deals," *Hypebot*, October 1, 2012, http://www.hypebot.com/hypebot/2012/10/spotify-adds-germanys-deutsche-telekom-to-growing-list-of-mobile-deals.html.

company pays for its own Internet connection, it instantly gets access to the whole global network – a virtually infinite addressable market. Small providers of content, applications, and services can compete directly for end users on a technologically neutral playing field, regardless of identity of the users' ISPs.

By contrast, if the Internet were to move in a direction where each ISP may determine whether and how fast its subscribers can access particular content and services, providers of online content and services would face a very different environment. Every new service would have to worry about how its traffic would be treated by various ISPs across the globe in order to be assured reaching the largest potential audience. And inevitably, some application providers would seek to gain competitive advantage by striking deals with ISPs for favorable treatment. As deals with ISPs became commonplace, anyone who did not strike such deals might face significant competitive disadvantages. Or in cases where paid priority was viewed as a necessity, content providers may choose to withhold their content from the customers of some access providers rather than pay. Whether through the onset of higher economic barriers to entry (such as a small startup in South America not having the leverage to pay to compete in foreign markets) or through refusals to serve certain markets deemed not worth the cost, the end result would be far fewer information sources and communications tools for Internet users.

Thus, the economic benefits of Internet neutrality – a neutral Internet that fosters competition among Internet-based services and economic development – also enhance the human rights benefits. By expanding the universe of information sources and services, this open, competitive environment supports user choice, free expression, access to knowledge and information, and public discourse and activism. The loss of a neutral platform for online services would undermine the ability of Internet users to fully exercise their fundamental rights online.

States' Role and Guiding Principles for Neutrality Rules

The Special Rapporteurs' Joint Statement on Freedom of Expression and the Internet, recognizing the Internet's power and the risk that interference with its use poses to free expression, included the following clear and specific call for the protection of Internet neutrality: "There should be no discrimination in the treatment of Internet data and traffic, based on the device, content, author, origin and/or destination of the content, service or application."22 Enacting laws or regulations to protect Internet neutrality is one step states can take to heed this call and meet their obligation to protect the right to freedom of expression and opinion as well as other rights empowered by the Internet.

For state-owned access providers or providers with relatively direct ties to government, disproportionate or egregious interference with citizens' use of the Internet may well rise to direct violations of users' rights under the ICCPR if they do not meet the standard for

[22] *See supra* note 13, ¶ 5.

permissible limitations.[23] But where Internet access services are privately run, even if competitively offered, discriminatory actions by these providers can also restrict rights. Indeed, the UN Special Rapporteur's report noted that "the private sector has gained unprecedented influence over individuals' right to freedom of expression."[24] And in such contexts where actions by private entities can restrict rights, the Human Rights Committee has advised that "the positive obligations on States Parties to ensure Covenant rights will only be fully discharged if individuals are protected by the State, not just against violations of Covenant rights by its agents, but also against acts committed by private persons or entities that would impair the enjoyment of Covenant rights in so far as they are amenable to application between private persons or entities."[25]

Below, we offer five principles to guide the substantive development of Internet neutrality protections that can help states meet their duty to protect free expression and other human rights online.

There should be a clear expectation that Internet access services must be provided in a neutral manner, without discrimination based on the content, applications, or services subscribers choose to access. The core principle of Internet neutrality is that ISPs must not discriminate among lawful traffic based on its content, source, destination, ownership, application, or service. There is an emerging consensus among states and regions that have taken up Internet neutrality to prefer application-agnostic, i.e. nondiscriminatory, network management.[26] Reasonable, narrow exceptions should be permitted, but non-discrimination –

[23] General Comment 34, *supra* note 14, ¶7 ("The obligation to respect freedoms of opinion and expression is binding on every State party as a whole. . . . Such responsibility may also be incurred by a State party under some circumstances in respect of acts of semi-State entities.") The UN Special Rapporteur's report, *supra note* 12, summarizes how, to be permissible under international human rights law, any such restrictions on free expression imposed by states must be (i) transparently described in law, and (ii) the least restrictive means of achieving a (iii) legitimate purpose as listed in Article 19.3 of the ICCPR.

[24] UN Special Rapporteur's Report, *supra note* 12, ¶ 44.

[25] UN Human Rights Committee, General Comment 31, *The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, Adopted 29 March 2004 (2187th meeting), ¶ 8, http://daccess-ods.un.org/access.nsf/Get?Open&DS=CCPR/C/21/Rev.1/Add.13&Lang=E; See also Human Rights Council, Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework,* March 21, 2011, (The Framework rests in part on states' obligation as to third parties, as well as the "corporate responsibility to respect human rights, which means that business enterprises should act with due diligence to avoid infringing on the rights of others.")

[26] *See*, e.g. US Federal Communications Commission, *Report and Order in the matter of Preserving the Open Internet* (GN Docket No, 09-191), Adopted 21 December 2010, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf; Canadian Radio-television and Telecommunications Commission, *Review of the Internet traffic management practices of Internet service providers* (CRTC 2009-657), 21 October 2009, http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm; Chile, Ley núm. 20.453 Consagra el Principo de Neutralidad en la Red para los Consumidores y Usarios de Internet, http://www.leychile.cl/Navegar?idNorma=1016570 (in Spanish); Netherlands, Telecommunications Act, adopted May 2012, discussion available at Door Ot van Daalen, "Netherlnds First Country in Europe with Net Neutrality," *Bits of Freedom blog*, 8 may 2012, https://www.bof.nl/2012/05/08/netherlands-first-country-in-europe-with-net-neutrality/ (partial unofficial English translation available at https://www.bof.nl/2011/06/27/translations-of-key-dutch-internet-freedom-provisions/; Solvenia, Zakona o

including banning both prioritization and de-prioritization of traffic – must be established as the baseline expectation.

The scope of the neutrality obligation should be clearly defined and should account for the crucial distinction between Internet access services and specialized services. CDT prefers the term "Internet neutrality" because the goal is to preserve the openness of the Internet – as opposed to other, non-Internet services that also may be offered using broadband networks, such as stand-alone voice- or television-over-IP services. The neutrality and openness of the Internet platform can be adequately protected without foreclosing the use those networks for a wide range of non-Internet services on terms and conditions of network operators' own choosing. But the line between Internet access and other services not subject to a neutrality obligation must be clear; specialized services must be truly specialized in the sense of serving a specific and limited purpose. A service that provides a general-purpose ability to send and receive data communications across the entire Internet should not be eligible for treatment as a specialized service.

The neutrality obligation should apply equally to fixed and mobile Internet access services. In a converging world where mobile wireless connectivity is expected to make Internet access increasingly ubiquitous, failing to address mobile would leave a gaping hole in any policy meant to promote openness and nondiscrimination on the Internet. Mobile carriers may face some special technical challenges, relating to such factors as spectrum limitations and radio interference. Given these technical realities, what constitutes reasonable traffic management on a mobile data network may differ from the norm on fixed connections. But there is no reason to think that mobile ISPs need to discriminate among traffic based on content-related factors such as its source, ownership, application, or service. Core neutrality principles can and should apply to mobile Internet access services.

There should be clear guidelines for evaluating exceptions for reasonable network management practices. Rather than attempting to specify which particular technical practices are acceptable, Internet neutrality rules should establish clear but flexible criteria for assessing the reasonableness of network management techniques that deviate from the non-discrimination norm. As exceptions to the neutrality rule, reasonable network management activities should be consistent with international human rights standards regarding transparency, narrow tailoring, and proportionality. Wherever possible, traffic management practices should be content- and application-neutral. This is the most reliable way to ensure that traffic management is applied fairly and evenly, and that the ISP is not selecting which specific content or applications to favor or disfavor. The US Federal Communications Commission, the Body of European Regulators for Electronic Communications, and the

---

elektronskih komunikacijah (ZEKom-1) (Electronic Communications Act), adopted 20 December 2012, http://www.uradni-list.si/_pdf/2012/Ur/u2012109.pdf#!/u2012109-pdf (English summary available at http://radiobruxelleslibera.wordpress.com/2013/01/03/slovenia-reinforces-net-neutrality-principles/.

French Autorité de Régulation des Communications éléctroniques et des Postes have all proposed criteria for assessing the reasonableness of network management practices[27].

The neutrality obligation should not apply to over-the-top services available on the Internet. Internet neutrality must focus on the goal of preserving the Internet as a neutral, non-discriminatory transmission medium. Thus, the obligation should apply to access providers only, and not to the limitless array of content, services, and application available over the Internet. Concerns over market power, competition, or the human rights impact and obligations of these services are best addressed separately.

*** * ***

As the role of the Internet in the social, economic, and political areas of everyone's life grows ever greater, states must act to ensure that the enjoyment of human rights is protected. We strongly believes that rules based on these principles will help preserve the Internet's unique power to promote free expression and other rights.

[27] FCC *Open Internet Order*, *ibid.*; ARCEP, *Internet and network neutrality: Proposals and recommendations,* September 2012, pp. 24–26, http://www.arcep.fr/uploads/tx_gspublication/net-neutralite-orientations-sept2010-eng.pdf; BEREC, *Summary of BEREC positions on net neutrality*, December 2012, p. 6, http://berec.europa.eu/files/document_register_store/2012/12/BoR_(12)_146_Summary_of_BEREC_positions_on_net_neutrality2.pdf.

Net Neutrality from a Public Sphere Perspective

by Francesca Musiani and Maria Löblich

Introduction

The Internet impacts social communication and the public sphere, and this impact has consequences for the political shape of the communication order – therefore, for society as a whole. One important question in this regard is which regulatory framework is being developed for the Internet, and how this framework enables and at the same time restricts communication in the public sphere. Net neutrality is at the very core of this question: distribution channels can be used as a means to discriminate, control, and prevent communication. In other words, content and user behavior can be controlled through the architecture of the physical layer and the "code" layer of the Internet. The discussion on net neutrality touches fundamental values (public interest, freedom of expression, freedom of the media, and free flow of information), that communications policy authorities in liberal democracies frequently appeal to in order to legitimize their interventions in media systems. The implementation of these values, from a normative point of view, is seen as the precondition for media to create the public sphere – be it online or offline – and thus fulfill its function in society (Napoli, 2001).

Differing concepts of the public sphere are present in the work of several authors. However, the concept developed by Jürgen Habermas (1989; Calhoun, 1992; Lunt & Livingstone, 2013; Splichal, 2012; Wendelin, 2011) is widely recognized as being the most influential. According to Habermas, the public sphere links citizens and power holders; it is "a realm of our social life in which something approaching public opinion can be formed." Habermas' concept of the public sphere centers on deliberation. Functioning deliberation requires that "access is guaranteed to all citizens" (Habermas, 1984, p. 49). This emphasis on access makes this concept of the public sphere particularly useful for an investigation of the net neutrality debate. Peter Dahlgren (1995, 2005, 2010) developed Habermas' notion of the public sphere into an analytic tool in order to study the role of the media and the Internet *vis-a-vis* the public sphere. According to Dahlgren, the public sphere is "a constellation of communicative spaces in society that permit the circulation of information, ideas, debates – ideally in an unfettered manner – and also the formation of political will" (Dahlgren, 2005, p. 148). Traditional media and online media play an important role in these spaces or "public spheres" (as there are distinct, sometimes overlapping social spaces that constitute different public spheres; Dahlgren, 2010, p. 21).

Dahlgren (1995) distinguishes three analytical dimensions of the public sphere: the structural, the representational, and the interactional. The structural dimension refers to the organization of communicative spaces "in terms of legal, social, economic, cultural, technical, and even Web-architectural features" (Dahlgren, 2005, p. 149). These patterns impact Internet access.

The representational dimension directs attention to media output and raises questions concerning fairness, pluralism of views, agenda setting, ideological biases, and other evaluation criteria for media content. According to Dahlgren, representation remains highly relevant for online contexts of the public sphere. The interactional dimension focuses on the ways users interact with the media and with each other in particular online sites and spaces. In these "micro-contexts of every-day life" users deliberate on meaning, identity, opinions, or entertain themselves (Dahlgren, 2005, p. 149).

We use these analytical dimensions as a heuristic framework to identify net neutrality areas that are relevant for communication studies; thus, each dimension serves as an entry point into a particular set of net neutrality issues. The structural dimension is an analytical starting point for examining the bundle of net neutrality issues that are related to access to the Internet infrastructure for individuals and collective entities. The representational dimension leads to the question of how net neutrality relates to online content. We refer to content "accessible in the public Internet," as opposed to secure or closed private networks (Marsden, 2010, p. 29). The related issues are content diversity, control, and censorship of social communication – although, of course, net neutrality is just one aspect of these debates. The interactional dimension directs attention to the modes, cultures, and spaces of social communication online and whether they are affected by net neutrality. Closed systems or "walled gardens" will illustrate the extent to which the potential benefits of online interaction and deliberation can be impeded or lost.

Dahlgren outlined these dimensions before the Internet became so widely diffused; thus, there is some overlapping when they are applied to online spaces. Content control carried out by Deep Packet Inspection (DPI) – packet filtering techniques examining the data and the header of a packet as it passes an inspection point in the network – may affect interacting users as much as media organizations. While Dahlgren pointed to the blurring of the representation and interaction dimensions in relation to the Internet, traditional mass communication categories such as "one-to-many" versus "one-to-one" can no longer be separated as clearly (Dahlgren, 2005, pp. 149-150). However, by distinguishing access to Internet infrastructure, diversity of content transmitted via Internet infrastructure, and user interaction enabled through Internet infrastructure, these dimensions provide important analytical tools.

Structural Dimension: Access to the Network for Content Producers

Architectural, economic, and other structures shape the organization of communicative spaces and constitute the framework for different actors' access to Internet infrastructure. Net neutrality bears technical implications and economic consequences for audiovisual content producers, news media outlets, and other corporate content providers. These implications influence the definition and the implementation of the quality of service principle. This principle is essential for audiovisual service providers because video on demand needs to be delivered by strict technical deadlines ("real-time" traffic). Delays severely and negatively affect the viewing experience (van Eijk, 2011, p. 9). By contrast, an email "just needs to get there as soon as (and as fast as) possible (so-called 'best-effort' traffic)" (Clark, 2007, p. 705).

Therefore, some authors make the point that network management can benefit content providers and consumers by making the flow of traffic more balanced, or smoother (Yoo, 2012, p. 542).

In order to prevent network overload at times of peak usage, corporate content providers make quality of service one of their priorities. Google has built its own infrastructure of server farms and fiber-optic networks in order to store content and get it more quickly to end-users (Levy, 2012). Economists have argued that producers of the next generation of online video, who depend "critically" on the prioritization of data, need a legal or quasi-legal assurance of their delivery (Hahn & Litan, 2007, p. 605). Proponents of net neutrality, however, emphasize that the priority should be to keep the costs of market entry as low as possible for the "lowest end market entrants – application companies" (Wu & Yoo, 2007, p. 591).

As the Internet becomes an increasingly important distribution channel for traditional media, the boundaries of old business models (television, telecommunication) blur. Problems arise with the interaction of content and networks (Vogelsang, 2010, pp. 8-9). In the view of many scholars, deviations from network neutrality do not necessarily harm users and media organizations. However, these scholars generally acknowledge that situations where Internet service providers become content providers may favor the implementation of network management techniques in order to discriminate against competitors. Providers can exclude competitor content, distribute it poorly, or make competitors pay for using high-speed networks (Marsden, 2010, p. 30; van Eijk, 2011, p. 10). Critics fear a similar model, derived from cable TV industry, where cable providers "charge a termination fee to those who wish to get access to the user" (Marsden, 2010, p. 18). In particular, this would mean a burden for new media businesses and non-commercial services, such as citizens' media and blogs. While large content providers are able to negotiate free or even profitable access, smaller content providers with less contracting power are forced to pay cable TV operators for access. As a result, net neutrality might be easily circumvented both by large content providers and ISPs (Marsden, 2010, pp. 18, 101). While some scholars argue that antitrust and competition laws are sufficient to protect upstart content providers from negative consequences of vertical integration and concentration (Hahn & Litan, 2007, p. 606), others argue that there are limits to competition in the access network market due to high fixed costs that restrict market entry (Vogelsang, 2010, p. 7).

In Europe, a special concern is public service broadcasting. Many scholars demand an open and non-discriminatory access to distribution for this service. Several German authors, for instance, regard must-carry rules as a suitable instrument to secure the circulation of online services: They suggest introducing a classification of online services that fulfill indispensable functions for public sphere, contribute to the diversity of opinions, and, therefore, should enjoy the privilege of must-carry rules. They classify public service broadcasting as such an indispensable service (Holznagel, 2010, p. 95; Libertus & Wiesner, 2011, p. 88). The question remains, however, who decides which services should get this privilege and, in general, whether net neutrality will only apply to public service broadcasting (directing other content into the slow lane) or to all content providers (Marsden, 2010, pp. 83, 98).

Representational Dimension: Diversity and Control of Content

A functioning public sphere is based on the representation of the diversity of information, ideas, and opinions (Dahlgren, 2005, p. 149). Different technical practices of inspection or prioritization of data packets, for political or law enforcement purposes, shape net neutrality in various ways. They condition access and circulation of content and restrict the variety and diversity of such content.

A number of technical practices are currently available to governments and the information technology industry to control or restrict content. Examples are bandwidth throttling (the intentional slowing down of Internet service by an ISP), blocking of websites, prioritization of certain services to the detriment of others, and Deep Packet Inspection (DPI). The latter has several implications, beyond net neutrality, for privacy, copyright, and other issues. DPI may be implemented for a variety of reasons, including the search for protocol non-compliance, virus, spam, intrusions; the setting of criteria to decide whether a packet may go through or if it needs to be routed to a different destination; and the collection of statistical information (Bendrath & Mueller, 2011; Mueller & Asghari, 2012).

As a technology capable of enabling advanced network management and user service and security functions potentially intrusive or harmful to user privacy – such as data mining, eavesdropping, and censorship – DPI has been framed in a predominantly negative way. This is due to the fact that, even though this technology has been used for Internet management for many years already, some net neutrality proponents fear that the technology may be used to prevent economic competition and to reduce the openness of the Internet. Indeed, this has already happened. For example, in April 2008, Bell Canada was accused of using DPI technology to block peer-to-peer traffic generated not only by clients of its service Sympatico but also by other consumers relying on independent ISPs (Bendrath & Mueller, 2011, p. 1153). Thus, net neutrality proponents argue that the purpose of DPI deployment is crucial and should be made as transparent as possible (Ufer, 2010). Furthermore, emphasis is put on the need to further reflect on the extent to which the employment of filtering techniques is bound to specific cultures. Blocking of content sometimes takes place in specific contexts where it is regarded to be harmful to the public or to some segment of the public, as is the case for hate speech. Some researchers warn that the role played by local values and cultures in the deployment of such measures should not be underestimated (Goldsmith & Wu, 2006; Palfrey & Rogoyski, 2006, p. 33). However, others emphasize instead that the implementation of these techniques, especially if bent to the requirements of political actors, may lead to biases in, blockings of, or censorship of the content of online communications. These scholars emphasize the power that ISPs have to "control access to vast expanse of information, entertainment and expression on the Internet" (Blevins & Barrows, 2009, p. 41; Elkin-Koren, 2006).

The intermediaries of the Internet economy have the technical means to implement traffic shaping practices, as well as a number of measures that are susceptible to affecting diversity of content on the Internet such as DPI or filtering. So far, the directive or mandate to shape traffic has often come from governments. The literature identifies two central motivations for

political actors adopting these practices. First, they may be used by authorities as an investigation tool. ISPs are sometimes used as "sheriffs" of the Internet, when they are placed in the position of enforcing the rules of the regime in which they are doing business (Palfrey & Rogoyski, 2006). The use of these measures is also attributed to security purposes such as the fight against terrorism, child pornography, online piracy – with all the controversies this raises in terms of setting critical precedents (Marsden, 2010, pp. 19, 67, 81) – or to allegedly protect largely shared values such as the protection of minors or the fight against hate speech (Marsden, p. 102). These techniques are also used for law enforcement in the area of intellectual property protection. For example, in the infamous Comcast controversy of 2007, one of the first controversies labeled as net neutrality-related, the U.S. broadband Internet provider started blocking P2P applications, such as BitTorrent. The stated rationale was that P2P is used to share illegal content and the provider's infrastructure was not designed to deal with the high-bandwidth traffic caused by these exchanges. Accordingly, the cinema and music recording industry have repeatedly taken positions against net neutrality in their fight against "digital piracy" (Bendrath & Mueller, 2011, p. 1152; Palfrey & Rogoyski, 2006, p. 45). Civil society organizations and some political actors have vocally opposed both these sets of motivations, deemed as inadequate to justify an increased control of data and the invasion of freedom of speech rights (Libertus & Wegener, 2011, p. 87).

Interactional Dimension: "Walled Gardens"

Net neutrality breaches also have effects on the interactional dimension of the public sphere. The formation, in the landscape of information and communication technologies, of so-called "walled gardens" – the carrier offers service without access to the wider Internet, controls applications, and restricts non-approved content – has important implications for online interaction and illustrates the extent to which the potential advantages leveraged through online interaction and deliberation can be short-circuited by restrictions on software and content (Marsden, 2010, p. 88).

The debate over the neutrality of the Internet is – perhaps surprisingly – often separated from a reflection on the attacks on the universality of the Web. However, the two largely overlap in the economic strategies of content providers and application designers on the Web and their effects on the network (Dulong de Rosnay, 2011). The tendency to create "walled gardens" is perhaps the best illustration of this phenomenon. For example, social networking services harness users' personal data to provide them with value-added services but exclusively and specifically on their own sites. In doing so, they contribute to the creation of sealed "silos" of information, and they do not allow users to export or recover data easily. The "giants" of digital services manifest, more and more frequently, their intention to become broad social platforms underpinning the entire spectrum of web services using these strategies. In fact, their goal is oftentimes to direct users to specific commercial services, to closed economic systems and stores that control not only the software that can be installed on users' devices but the content (Zittrain, 2008).

This is an issue of both application discrimination and content discrimination (Marsden, 2010,

p. 88). The ways in which content providers rely on applications that depend on major social networking players reinforces this logic of partition and gate-keeping. The walled gardens phenomenon has also been described as "balkanization" or "gilded cages." Hardware manufacturers also seek to ensure a "captive audience": The model proposed by Apple, notably, forbids providers of content and media to directly propose applications to users and prevents them from buying paid goods, such as music or digital books, outside of the Apple ecosystem (which includes, e.g., a partnership with Amazon).

Breaches of neutrality also affect the application layer itself. Carriers "offer exclusive, preferential treatment to one application provider," thereby creating walled gardens of preferred suppliers (Marsden, p. 88). Search engines choose their answers to queries based on advertising revenue, while endorsement systems such as "Like" on Facebook and "+1" on Google, and social networking/recommendation systems such as the now defunct Ping for iTunes, form a set of competing systems that affect the entire value chain of the Internet. The issue of "exclusivities" – especially in the mobile Internet – and of the mergers between communication operators and other stakeholders, such as Deezer and Orange, are further symptoms of the emergence of vertical conglomerates.

The walled gardens phenomenon, as an illustration of the interactional dimension of the public sphere, bridges the structural and representational dimensions by revealing the close connection between the diversity of content and the "diversity of stakeholders who have editorial control over that content" (Herman, 2006, p. 116). The policy implemented by Apple in relation to applications developed by external actors is seen as a possible way to downplay unwelcome political and cultural ideas. Preventing an application from running on Apple devices may have immediate implications for diversity of political views. Similarly, an ISP may or may not allow users to select some of the Web sites contained or barred from the garden, thus hindering expressions of political and social significance with network management choices (Nunziato, 2009, pp. 5-8). The isolation of content on specific networks or services from other content on the wider Internet, preventing broader interaction between them, is reinforced by the "cumulative effect" of walled gardens. If a sufficient number of people join a service and the service is able to reach a critical mass of users, the system becomes self-reinforcing. The companies managing them are able to move toward a quasi-monopoly (Marsden, 2010, pp. 67, 186-194).

Legal scholar Christopher Yoo argued that ISPs and companies such as Apple may be considered as editors, endowed with "editorial discretion" and equipped with "editorial filters," because of their *de facto* right to remove inappropriate content (2005, pp. 47-48). He controversially points out that "the fact that telecommunications networks now serve as the conduit for mass communications and not just person-to-person communications greatly expands the justification for allowing them to exercise editorial control over the information they convey. In the process, it further weakens the case in favor of network neutrality" (Yoo, 2005, pp. 47-48). In this view, net neutrality measures would be counter-beneficial as they would prevent ISPs from providing some guarantee of quality of content, when faced with information overload. For example, Blevins and Barrows (2009) stated that "certain ISPs may

not want to carry speech that in their determination is indecent, pornographic, or related to hate groups or particular religious or political persuasions" (p. 38). However, the comparison made by Yoo with editorial rights of newsrooms (2005, pp. 46-47) appears inadequate, as journalism is a profession with its own logic, self-understanding, norms, rules, and programs, which do not apply to ISPs. Herman (2006) pointed out that broadband providers are not considered to be editors. In addition, giving editorial control to users of the Internet, rather than providers, best exemplifies democratic goals (Blevins & Barrows, 2009, p. 41).

The issue of walled gardens and net neutrality is further compounded (and complicated) by the advent of the mobile Internet, for which the allotted bandwidth remains scarce. At the same time, mobile networks increasingly constitute the first "entry point" into the Internet for several regions in the world – first and foremost, Africa. Access restrictions on mobiles to certain protocols, such as Voice over IP (VoIP), and other limits, are officially justified by a poor allocation of band frequency. But they are often attributable, behind the scenes, to industrial battles. The model fostered by Apple's iPhone (and its "cousins", such as Amazon's Kindle tablet) contributes to the change in the market's power relations, by contributing to the shift of power from the operator to the hardware manufacturer (Curien & Maxwell, 2011, p. 64).

Many of the most recent attempts to circumvent net neutrality directly involve mobile telephony. In the summer of 2010, Google and Verizon were discussing the prices that the "giant" of search would have to pay to the operator for a "preferential treatment" given to the videos of Google's subsidiary YouTube. The reasons why Google – previously very much in favor of Internet providers' independence – changed its position are numerous, but the first and foremost is the ongoing battle between Google's Android and Apple's iPhone. By blocking some of Google's applications – notably a system allowing to telephone via the Internet rather than the mobile network, and the applications for geo-localized advertisement – Apple has shown the force of a system installed behind a steely wall of exclusivity. Also, in order to be diffused on the iPhone, YouTube's videos need to be encoded in the H264 format, for which Apple has patents. Google has now replied with the WebM format, bought from On2 Technologies and transformed into an open web media project. The speed at which YouTube became the primary video streaming service on the Internet may reinforce this tendency to WebM, which has become the standard on all Chrome and Firefox navigators since April 2011. This battle between Google and Apple shows how, even if there is a diversity of applications serving the same end, the lack of openness of such applications limits interaction, at best, to within each of them, thereby greatly reducing interoperability and access.

The danger of these power plays has not gone unnoticed by scholars. Interviewed by the *New York Times* on November 14, 2010, Tim Wu – whose then-recently published book *The Master Switch* described the rise-and-fall cycles of great "communication empires" (Wu, 2010) – gave a disenchanted view of the Cupertino firm and its now-deceased CEO Steve Jobs, noting that "firms today, like Apple, make it unclear if the Internet is something lasting or just another cycle . . . The man who helped create the personal computer 40 years ago is

probably the leading candidate to help exterminate it. His vision has an undeniable appeal, but he wants too much control" (Wu & Bilton, 2010).

Conclusions

Net neutrality is concerned with the organization of the online public sphere infrastructure, in particular its technical, and especially its economic and power structures. At the same time, net neutrality takes into account the interests of old and new content providers and of Internet users and Internet service providers. Large content providers such as Google and Facebook are not the only "gatekeepers" in the Internet. Internet service providers, perhaps more than any other entity, enable and constrain online communication. Net neutrality research takes their position into consideration, exploring how diverse interests can be balanced in the light of increased bandwidth usage, quality of service demands, and limited mobile Internet capacities.

A functioning public sphere is based on the representation of the diversity of information, ideas, and opinions. Traffic shaping and filtering measures are applied for economic reasons, but also for political and law enforcement ones. These measures can be fostered by other actors than Internet service providers.

The existence of "walled gardens" points to the fact that interaction in the online public sphere can be impeded by restrictions on software and content. In closed platforms, providers decide which applications, content, and information are allowed and which are not allowed within the service. Proprietary, closed systems set limits for connecting to the Web and pose limits to the user's individual capacity to refine or develop new applications based on existing ones. Users, when confronted to the net neutrality debates, are equipped with diverse and uneven tools. Not all users have the technical knowledge enabling them to make informed choices; these are therefore, out of necessity, often left outside the realm of political intervention and to the exclusive authority of the market. Thus, actors with large and multifaceted stakes in the Internet value chain are constantly on the verge of monopolizing a debate with underlying impacts on social architecture, fundamental freedoms, and the conditions for democratic expression.

There is some overlapping and interrelation between the dimensions, due to the blurring of categories in an online public sphere. However, the three analytical dimensions – access to Internet infrastructure, diversity of content transmitted via Internet infrastructure, and user interaction enabled through Internet infrastructure – highlight how a perspective grounded in communication studies can complement the frameworks offered in the economic and legal traditions, thereby offering a more robust basis for an informed debate on the issues raised by the contested net neutrality terrain. The public sphere perspective connects, for example, scholars interested by freedom of expression and speech with those concerned by issues of economic advantage, monopoly, and concentration. Several fundamental issues central to communication studies, which have been re-labeled as net neutrality – for example network (de-)centralization, bottleneck regulation, monopoly and competition, public service values – reappear in new forms in the Internet environment.

References

Bendrath, R. & Mueller, M. (2011). The end of the net as we know it? Deep packet inspection and Internet governance. *New Media & Society*, *13*, 1142-1160. http://dx.doi.org/10.1177/1461444811398031

Blevins, J. & Barrow, S. (2009).The political economy of free speech and network neutrality: A critical analysis. *Journal of Media Law & Ethics, 1*(1/2), 27-48.

Calhoun, C. (ed.) (1992). *Habermas and the Public Sphere*. Cambridge, MA: MIT Press.

Clark, D. (2007). Network neutrality: Words of power and 800-pound gorillas. *International Journal of Communication, 1,* 701-708.

Curien, N. & Maxwell, W. (2011).*La neutralité d'Internet*. Paris: La Découverte.

Dahlgren, P. (1995). *Television and the Public Sphere*. London: Sage.

Dahlgren, P. (2005). The Internet, public spheres, and political communication: Dispersion and deliberation. *Political Communication, 22*, 147-162. http://dx.doi.org/10.1080/10584600590933160

Dahlgren, P. (2010). Public spheres, societal shifts and media modulations. In J. Gripsrud & L. Weibull (Eds.), *Media, markets & public spheres. European media at the crossroads* (pp. 17-36). Bristol: Intellect.

Dulong de Rosnay, M. (2011). Réappropriation des données et droit à la rediffusion. *Hermès, 59*, 65-66.

Elkin-Koren, N. (2006). Making technology visible: Liability of internet service providers for peer-to-peer traffic. *New York University Journal of Legislation & Public Policy, 9* (15), 15-76.

Goldsmith, J. & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world.* Oxford: Oxford University Press.

Habermas, J. (1984).*The theory of communicative action* (Vol. I & II).. Cambridge: Polity Press.

Habermas, J. (1989). *The structural transformation of the public sphere*. Boston: MIT Press

Hahn, R. & Litan, R. E. (2007). The myth of network neutrality and what we should do about it. *International Journal of Communication, 1,* 595-606.

Herman, B. D. (2006): Opening bottlenecks: On behalf of mandated network neutrality. *Federal Communications Law Journal,59*, 107-159.

Holznagel, B. (2010). Netzneutralität als Auf gabeder Vielfaltssicherung. *Kommunikation und Recht, 13*, 95-100.

Levy, S. (2012, November). Power House. Deep inside a Google data center. *Wired*, 174-181.

Libertus, M. & Wiesner, J. (2011). Netzneutralität, offenes Internet und kommunikative Grundversorgung. *Media Perspektiven,2*, 80-90.

Lunt, P. & Livingstone, S. (2013). Media studies' fascination with the concept of the public sphere: Critical reflections and emerging debates. *Media Culture & Society,35*, 87-96. http://dx.doi.org/10.1177/0163443712464562

Marsden, C. (2010). *Net neutrality. Towards a co-regulatory solution.* London: Bloomsbury Academic http://dx.doi.org/10.5040/9781849662192

Mueller, M. & Asghari, H. (2012). Deep packet inspection and bandwidth management: Battles over BitTorrent in Canada and the United States. *Telecommunications Policy, 36*, 462–475. http://dx.doi.org/10.1016/j.telpol.2012.04.003

Napoli, P. (2001). *Foundations of communications policy: Principles and process in the regulation of electronic media*. Cresskill, NJ: Hampton Press.

Nunziato, D. (2009). *Virtual Freedom: Net neutrality and free speech in the Internet Age*. Stanford: Stanford University Press.

Palfrey, J. & Rogoyski, R. (2006). The move to the middle: The enduring threat of "harmful" speech to network neutrality. *Washington University Journal of Law and Policy, 21*, 31-65.

Splichal, S. (2012). *Transnationalization of the Public Sphere and the Fate of the Public.* New York: Hampton Press.

Ufer, F. (2010). Der Kampf um die Netzneutralität oder die Frage, warum ein Netz neutral sein muss. *Kommunikation und Recht,13*, 383-389.

Van Eijk, N. (2011). Net neutrality and audiovisual services. *Iris plus*, 2011-5, 7-19.

Vogelsang, I. (2010). Die Debatte um Netzneutralität und Quality of Service. In D. Klumpp, H. Kubicek, A. Roßnagel & W. Schulz (Eds.), *Netzwelt – Wege –Werte – Wandel (*pp. 5-14). Berlin: Springer. http://dx.doi.org/10.1007/978-3-642-05054-1_1

Wendelin, M. (2011). *Medialisierung der Öffentlichkeit. Kontinuität und Wandel einer normativen Kategorie der Moderne*. Köln: Halem.

Wu, T. (2010). *The master switch: The rise and fall of information empires.* New York: Knopf.

Wu, T. & Bilton, N. (2010, November 14). One on one: Tim Wu, author of 'The Master Switch' [Web log post]. Retrieved from: http://bits.blogs.nytimes.com/2010/11/14/one-on-one-tim-wu-author-of-the-master-switch/

Wu, T. & Yoo, C. S. (2007). Keeping the Internet Neutral?:Tim Wu and Christopher Yoo Debate. *Federal Communications Law Journal, 59*, 575-592.

Yoo, C. S. (2005). Beyond network neutrality. *Harvard Journal of Law & Technology*, 19, 1-77.

Yoo, C. S. (2012). Network neutrality and the need for a technological turn in Internet scholarship. In M. E. Price, S. G. Verhulst & L. Morgan (Eds.), *Routledge handbook of media law* (pp. 539-555). New York, Abingdon: Routledge.

Net Neutrality:
Ending Network Discrimination in Europe

by Raegan MacDonald and Giusy Cannella

Introduction

The internet's continuing success rests on its three foundational principles: 1) that all points in the network should be able to connect to all other points in the network (the *end to end principle*); 2) that all providers of the internet should make their best effort to deliver traffic from point to point as expeditiously as possible (the *best effort principle*); and 3) that everyone should be able to innovate without permission from anyone or any entity (the *innovation without permission principle*). Collectively, these principles are the foundation of the openness and neutrality of the internet.

In practice, this means that Internet Service Providers[1] (hereafter ISPs) must treat all internet traffic on an equal basis, no matter the origin or type of content or means (equipment, protocols, etc) used to transmit packets, leading to the term "network neutrality." Yet, every day, ISPs are violating these principles, engaging in what is effectively network discrimination, that is – as elaborated upon in this paper - discrimination that ISPs apply on traffic on the network.
In May 2012, the Body of European Regulators for Electronic Communications (BEREC) published the findings of a joint investigation with the European Commission regarding traffic management. It revealed an increased trend of operators restricting access to services and sites. The most frequently reported restrictions are the blocking and/or throttling of peer-to-peer (P2P) traffic, on both fixed and mobile networks, and the blocking of internet telephony (Voice over IP), mostly on mobile networks[2].
Access[3] strongly believes that the only way to stop arbitrary discrimination online is to enact legislation enshrining network neutrality in law. Around the world there have been few, but, significant legislative initiatives to codify network neutrality. In 2010, Chile[4] was the first country to adopt legislation explicitly laying out network neutrality principles, followed by

[1] By "Internet Service Providers" (ISPs) we are referring to companies that provide internet access to the public, sometimes called "internet access providers". Many but not all of ISPs are telephone companies or telecommunications providers.
[2] BEREC/European Commission, A view of traffic management and other practices resulting in restrictions to the open Internet in Europe - Findings from BEREC's and the European Commission's joint investigation, 2012, BoR (12) 30, 29th May 2012: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf.
[3]Access (AccessNow.org) is an international NGO that defends and extends the digital rights of users at risk around the world. Combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.
[4]Bill 4915: Amendment to the Chilean Telecommunications Act: http://www.camara.cl/prensa/noticias_detalle.aspx?prmid=38191.

the Netherlands[5] which, in 2011, became the first European Union Member State to guarantee that "providers of public electronic communication networks which deliver internet access services and providers of internet access services do not hinder or slow down applications and services on the internet." In 2012, Slovenia[6] also enshrined the fundamental principle of net neutrality in law, and other countries – such as Brazil, Germany and France – are currently moving in the same direction. We strongly urge the European Union to follow their examples and thereby ensure that net discrimination does not occur in any Member State.

The purpose of this paper is to provide more detailed insight into the issues surrounding the network neutrality debate in the European context. As this debate is often highly technical and subject to many misunderstandings, this paper will provide a brief clarification on some of these main topics, particularly the definition of network discrimination, what constitutes "reasonable" traffic management and its impacts on the economy and the fundamental rights to privacy, data protection, and freedom of expression.

Benefits of net neutrality

As of June 2012, more than 2.7 billion people[7] – over a third of the world's population – have access to the internet, with more than 600,000 new users connecting each and every day[8]. These figures are particularly substantial if we look at the European Union where, of 500 million inhabitants, 67.5% of the population is connected to "the network of networks"[9].

Unfettered access to the internet is becoming recognised as a basic human right[10]. Frank la Rue, UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, has underlined the fact that the internet is a gateway through which fundamental rights can be realised, notably the freedoms of expression and association, but also the rights to access culture and education[11]. Furthermore, an open and neutral internet – without discriminatory interference of any sort – safeguard the fundamental rights to privacy and data protection.

[5]Summary from Bits of Freedom of the amended Dutch Telecommunications Act: https://www.bof.nl/2011/06/27/translations-of-key-dutch-internet-freedom-provisions/.

[6] Innocenzo Genna, Slovenian reinforces net neutrality principles, radiobruxellaslibera, 30 January 2013: http://radiobruxelleslibera.wordpress.com/2013/01/03/slovenia-reinforces-net-neutrality-principles/.

[7]International Telecommunication Union: The World in 2013 - ICT Facts and Figures: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigu13.pdf. res20

[8]Infographic on internet usage, Royal Pingdom, 2012: http://royal.pingdom.com/2012/02/16/almost-8-new-internet-users-added-worldwide-every-second-infographic/

[9]European Commission, 2012, Digital Agenda Scoreboard 2012: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/scoreboard_life_online.pdf.

[10] The Atlantic 2011, United Nations Declares Internet Access a Basic Human Right: http://www.theatlantic.com/technology/archive/2011/06/united-nations-declares-internet-access-a-basic-human-right/239911/.

[11] UN General Assembly, 17th Session, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, No. 27 (A/HRC/17/27), Official Record, Geneva, 2011: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

The importance of an open and neutral internet has also been recognised by several respected institutions: from the Council of Europe,[12] and the OECD,[13] to the World Bank, for the exercise of human rights, and also as a platform for economic growth. In particular, a World Bank report reveals that there is a direct correlation between the increase of high speed internet connection and development across all levels of the economy and society[14].

In 20 years, the digital market has become quite possibly the greatest driver for job creation, innovation, and competitiveness the world has ever known. This has been possible thanks to an open and neutral platform allowing web entrepreneurs to enter the market and innovate with groundbreaking ideas.

In a joint letter[15] delivered at a June 2013 event in the European Parliament organised by Access[16] to discuss the importance of network neutrality, a coalition of 20 European startups asked EU Commissioner for the Digital Agenda Neelie Kroes to keep the internet open and neutral so they can continue to innovate "without permission" of ISPs that may want to play the role of gatekeepers.

However, internet access services in Europe are frequently discriminatory, a practice that must be stopped if fundamental rights are to flourish and the economic benefits of the Digital Single Market are to be realised.

What is network discrimination?

Access defines "network discrimination"[17] as the tendency of ISPs to intentionally and arbitrary apply restrictions to users' access to the open and neutral internet. Generally speaking, network discrimination can take place, *inter alia*, in the following ways:

a. **Blocking of applications and services**: In order to maximise profits, some ISPs that also offer their own services and applications online, exclude certain services and applications of competing market players. The most prominent case of this form of network discrimination is European mobile providers (like Deutsche Telekom)

[12]Council of Europe, 2011, Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet: https://wcd.coe.int/ViewDoc.jsp?id=1835707.
[13] OECD Input to the United Nations Working Group on Internet Governance (WGIG), 2005: http://www.oecd.org/sti/ieconomy/e-bookoecdinputtotheunitednationsworkinggrouponinternetgovernance.htm#pro.
[14]World Bank Group, Summary of the 2009 World Bank Group Report here: http://web.worldbank.org/WBSITE/EXTERNAL/NEWS/0,,contentMDK:22231347~pagePK:34370~piPK:34424~theSitePK:4607,00.html.
[15]Open Letter by European CEO to the European Commission: http://www.reddit.com/r/POLITIC/comments/1fn1r7/net_neutrality_open_letter_by_european_ceos_to/.
[16] Schaake Marietje, 2013, Guaranteeing competition and the open internet in Europe, program and video of the full event here: http://www.marietjeschaake.eu/livestream-guaranteeing-competition-and-the-open-internet-in-europe/.
[17] Access, 2013, Q&A on Network discrimination in Europe, Access: https://s3.amazonaws.com/access.3cdn.net/b4f8ee73a73517829c_sam6b8g51.pdf.

blocking or restricting the use of Voice over IP (VoIP) services (like Skype and Viber) for their customers[18].

b. Slowing or "throttling" internet speeds: Some ISPs slow down specific services (like YouTube) and applications (like Skype), or ask users to pay an extra fee to have access to these internet platforms. Given the high latency (delay) sensitivity of many applications, ISPs are able to compromise the correct functioning of these services by slowing them down, preventing the services from running properly. Often ISPs – especially telecommunication companies – do this to favour their own voice calling services over VoIP services, thereby crushing competition.

c. Blocking websites: ISPs often block websites for a number of reasons – to secure their network, or to avoid competition, and sometimes for social, public relations or political reasons.

d. Preferential treatment of services and platforms: ISPs can also impose data caps on internet access contracts while granting data allowance exceptions to a company's own proprietary streaming services (like Deutsche Telekom to its own "T-Entertain")[19]. They can (and do) also grant preferential treatment to select services – such as Orange France with the popular music streaming service Deezer[20] – ahead of other competitors, effectively imposing anti-competitive limitations on markets such as those for legal online music. Moreover, generally only large, well-established companies can afford this preferential treatment, resulting in a further stifling of innovation.

What is "reasonable" traffic management?

Discriminatory practices are often justified by ISPs[21] as "reasonable" traffic management implemented to limit congestion on their networks. However, there is a fine line between preventing saturation by slowing down or throttling certain streams and degrading the quality of competing services. This leads to another question in this debate: what do acceptable traffic management practices look like?

[18]Information Week, 2009, Deutsche Telekom Restricts Skype On iPhone: http://www.informationweek.com/personal-tech/smart-phones/deutsche-telekom-restricts-skype-on-ipho/216402527.

[19]Gigaom, 2013, Deutsche Telekom's "anti-net-neutrality" plans alarm German government: http://gigaom.com/2013/04/25/deutsche-telekoms-anti-net-neutrality-plans-alarm-german-government/.
Plum Consulting, 2011, The open internet – a platform for growth – A report for the BBC, Blinkbox, Channel 4, Skype and Yahoo: London, p. 19: http://www.plumconsulting.co.uk/pdfs/Plum_Oct11_The_open_internet_-_a_platform_for_growth.pdf.

[20] Cable.co.uk, 2011, Orange partners with Spotify rival Deezer: http://www.cable.co.uk/news/orange-partners-with-spotify-rival-deezer-800721617/.

[21] Plum Consulting, 2011, The open internet – a platform for growth – A report for the BBC, Blinkbox, Channel 4, Skype and Yahoo: London, p. 19: http://www.plumconsulting.co.uk/pdfs/Plum_Oct11_The_open_internet_-_a_platform_for_growth.pdf.

Traffic management is "reasonable" when it is deployed for the purpose of technical maintenance of the network, namely to block spam, viruses, or denial of service attacks, or to minimise the effects of congestion, whereby equal types of traffic should be treated equally – as established by the Dutch net neutrality law. Traffic management techniques should only be used on a temporary basis, during exceptional moments.

When traffic management practices are put in place to pursue other purposes or are used on a permanent basis, they should be considered as unreasonable. Furthermore, discriminatory practices – such as blocking and throttling competing services should be clearly prohibited by law as they threaten citizens' fundamental rights and undermine the proper functioning of the online marketplace.

However, many ISPs claim that the exponential growth in web usage, particularly bandwidth intensive video applications, along with the alleged rise in infrastructure costs, cause congestion on the network and that without a degree of traffic management; congestion would make it impossible for users to enjoy sufficient quality of service. In response to the alleged "data explosion"[22], ISPs are making greater use of traffic management techniques in order to provide "guaranteed quality of service," which is the ability to provide different priority to different applications, services, or data. However, guaranteeing a certain quality of service to the detriment of other types of data, applications, services, etc., at their sole discretion is a violation of the best effort principle, and therefore can not be defined as reasonable traffic management.

Access believes that allowing ISPs to offer guaranteed quality of service exclusively to one or more applications within a class of applications (for example between VoIP applications) should be prohibited[23]. Indeed, this type of preferential treatment interferes with users' ability to use the applications and services of their choice without interference from ISPs. It also enables these latter to use the provision of quality of service as a tool to distort competition among applications within a class, which is exactly what network neutrality would safeguard against.

The Body of European Regulators for Electronic Communications (BEREC) has recognised that quality of service guarantees are simply not needed. A recent BEREC report points out that: "While not providing a guaranteed quality level of data delivery, the best effort approach of the internet does not imply low performance, and in fact results in most cases in a high quality of experience for users, even for delay-sensitive applications such as VoIP"[24].

[22] Analysys Mason, 2012, The collapse in the value if the mobile and gigabyte: myth and reality: http://www.analysysmason.com/About-Us/News/Insight/Insight_collapse_value_GB_Jan2012/#.UjNAY5Vzpd2.

[23] Access, 2012, Telco Action Plan – Respecting Human Rights: Ten steps and implementation objectives for telecommunication companies: ttps://s3.amazonaws.com/access.3cdn.net/1f9ab2891a86f3f081_uom6iil1w.pdf.

[24] BEREC, 2012, BEREC's comments on the ETNO proposal for ITU/WCIT or similar initiatives along these lines: http://berec.europa.eu/files/document_register_store/2012/11/BoR_(12)_120_BEREC_on_ITR.pdf.

While we agree that ISPs should be able to manage their networks, we believe traffic management should only be allowed as narrowly tailored deviations from the rule, and should not include arbitrary or permanent restrictions by ISPs, as these practices go clearly against the "end-to-end" and "best effort" principles that are fundamental to the internet's functioning. In the end, the best way ISPs can manage traffic is to invest in network infrastructure to increase the networks' capacity and avoid congestion.

What are the fundamental rights impacts of filtering technologies?

The increasing use of perpetual and unjustified traffic management also raises questions about privacy of communications. In order to implement a variety of traffic management practices, such as blocking, shaping, or filtering, several ISPs deploy tools such as Deep Packet Inspection (DPI)[25], a technology that allows them to examine data traveling over the internet and recognise what sort of packet it is – a virus or simply an email, for example – and therefore to interfere with such communications.

Although DPI is often used by ISPs to detect and mitigate attacks to their networks (e.g. a virus or other malicious software), this technology can also be deployed for reasons that fall far outside the scope of securing the network. Indeed, this highly intrusive tool can be used not only to implement discriminatory practices – such as blocking or prioritisation of certain types of traffic – but also to monitor and even copy all information that travels across a network. This is not a hypothetical, it happens everyday in countries like China, Iran, and Russia – whose governments frequently deploy this technology to censor political speech and suppress dissenting activity online[26]. It is also implemented in democratic countries such as Germany and the United Kingdom[27].

By inspecting communications data, ISPs may breach the privacy of communications, which is a fundamental right guaranteed by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. In line with the opinion of the European Data Protection Supervisor, these filtering techniques must only be used "in conformity with the

[25] Deep Packet Inspection (DPI) is a computer network surveillance technique that uses device and technologies that inspect and take action based on the contents of the packet i.e. it consider the complete payload of packet rather than just the packet header (definition from the Institute of Electrical and Electronics Engineers (IEEE). See paper here: http://ieeexplore.ieee.org/xpl/login.jsp?reload=true&tp=&arnumber=5772430&url=http://ieeexplore.ieee.org/xpls/abs_all.jsp%3Farnumber%3D5772430.

[26] Privacy International, 2012, The Kremlin's new Internet surveillance plan goes live today: https://www.privacyinternational.org/blog/the-kremlins-new-internet-surveillance-plan-goes-live-today.

[27] Open Rights Group, 2013, quick guide to Cameron's default Internet filters: https://www.openrightsgroup.org/blog/2013/a-quick-guide-to-camerons-default-internet-filters.

applicable data protection and privacy safeguards, which lay down limits as to what can be done and under which circumstances"[28].

The Dutch net neutrality law, the first of its kind in Europe, does an exemplary job addressing this. This law not only prohibits ISPs from throttling or filtering the connections of their customers, it also provides strict guidelines on the techniques that can be employed for unjustified traffic management (and wiretapping). Specifically, the use of filtering software as an advanced surveillance tool – which would include Deep Packet Inspection – is prohibited without the express consent of the user or the company being served with a valid legal warrant.

The current state of play in the European Union

Since the summer of 2010 the European Commission has launched two public consultations to explore issues of internet traffic management, but despite the evidence revealed by BEREC's investigations, no concrete actions have been undertaken to prevent network discrimination.

At the end of 2012 the European Parliament adopted two resolutions supporting the need for legislation that would enshrine net neutrality in order to ensure the completion of the European Digital Single Market[29].
The European Commission is currently looking to publish its "**Recommendations on the Open Internet and Network Neutrality**" by the end of 2013/early 2014, which according to the Commission's website will include guidance on transparency, elements of traffic management, switching, and the responsible use of traffic management tools[30].

In parallel, the European Commissioner for the Digital Agenda Neelie Kroes has recently issued a proposal for a **Regulation for a Telecoms Single Market[31]** that includes binding measures for the telecoms sector to achieve the Commission's goal of a "Connected Continent." However, while according to the Commission's press release[32] the proposed

[28] EDPS, 2011, Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data: http://ec.europa.eu/bepa/european-group-ethics/docs/activities/peter_hustinx_presentation_(1)_15_rt_2011.pdf.
[29]European Parliament, Committee on the Internal Market and Consumer Protection, 2012, Report on Completing the Digital Single Market (2012/2030(INI)), A7-034/2012, 26.10.2012, here: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2012-0341+0+DOC+PDF+V0//EN and Report on a Digital Freedom Strategy in EU Foreign Policy (2012/2094(INI), A7-0374/2012, 15.11.2012, here: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2012-0374+0+DOC+PDF+V0//EN&language=EN.
[30]European Commission, Digital Agenda for Europe, Open Internet: https://ec.europa.eu/digital-agenda/en/eu-actions.
[31] European Commission, 2013, Proposal for a regulation of the European Parliament and of the Council, laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012, COM(2013) 627 final: http://ec.europa.eu/transparency/regdoc/rep/1/2013/EN/1-2013-627-EN-F1-1.Pdf.
[32] European Commission, 2013, Commission proposes major step forward for telecoms single market, release: http://europa.eu/rapid/press-release_IP-13-828_en.htm.

Regulation will "encourage more competition between more companies" and guarantee "net neutrality, innovation and consumer rights", it fails to deliver on a number of fronts. Below we will highlight some of the major concerns.

Although the legislative text contains provisions (Article 23) that would prohibit access providers to "block, slow down, degrade or otherwise discriminating against specific services, content or applications," it makes these provisions meaningless by allowing internet access providers to enter into commercial agreements with big content providers in order to prioritise internet traffic. One of the most problematic outcomes of such special deals is that big content providers would be able to enter into commercial deals with access providers to ensure that their traffic is always delivered first and faster.

Furthermore, the Regulation would allow access providers to impose "data-caps" on internet access contracts while granting priority to their own services (like Deutsche Telekom to its own "T-Entertain")[33]. In this way, access providers grant preferential treatment to selected services, while competitors' services are discriminated against, effectively imposing anti-competitive limitations on online markets and leading to a "two-tier internet." The sum of these provisions would equal the exact opposite of net neutrality.

Indeed, Commissioner Kroes, once a strong proponent of network neutrality[34], seems to have abandoned her commitment to ensure an open and neutral internet. Her approach, which is now confirmed in the proposed Regulation, has wavered in speeches between bold statements stating her desire to ensure that all EU citizens have access to an open and neutral internet[35], while at other times suggesting that a sufficient solution to such pervasive discrimination would be to compel telecommunication companies to be transparent[36] so citizens can make "informed choices"[37]. This suggests that as long as telecommunication companies disclose whether or not they apply restrictions on internet usage, they can act discriminatorily. According to this logic, such transparency will enable users to "switch" service providers and internet offers "without countless obstructions" if they are not getting the full internet they expect.

This approach problematically suggests that competition and enhanced transparency might be sufficient to protect net neutrality. But transparency and "switching" are simply not a solution

[33] Gigaom, 2013, Deutsche Telekom's "anti-net-neutrality" plans alarm German government: http://gigaom.com/2013/04/25/deutsche-telekoms-anti-net-neutrality-plans-alarm-german-government/.
[34] Tiki-Toki, EDRi's timeline here: http://www.tiki-toki.com/timeline/entry/108784/Net-neutrality-in-Europe/#vars!date=2010-01-11_04:39:29!.
[35] Kroes, Neelie, The politics of the completing the telecoms single market, 30th May 2013, SPEECH/13/484: http://europa.eu/rapid/press-release_SPEECH-13-484_en.htm.
[36] Libération, 2013, Internet et applications de filtrage: une histoire de choix et de recettes, 16th January 2013: http://www.liberation.fr/medias/2013/01/16/internet-et-applications-de-filtrage-une-histoire-de-choix-et-de-recettes_874443.
[37] Kroes, Neelie, The EU, safeguarding the open internet for all, 4th June 2013, SPEECH/13/498: http://europa.eu/rapid/press-release_SPEECH-13-498_en.htm.

if there is no real competition in the market[38]. These elements will not effectively guarantee the freedom to impart and receive information the way an open and neutral internet provides.

The proposed Regulation has already been the subject of heated debate, even within the European Commission, as revealed by EDRi in a leaked internal Commission document[39]. In particular, DG Justice raised concerns that the Regulation could undermine the Charter of Fundamental Rights, namely freedom of expression. The document also warned of the dangers of encouraging preferential agreements between content and access providers.

The Commissioner for Enterprise and Industry is equally concerned that such an undermining of net neutrality would have an adverse effect on EU entrepreneurs, an element ironically highlighted by Commissioner Kroes herself only a few short months ago[40].

A Commission's internal vote showed that Commissioner Kroes' proposal did not have the support of a large majority of Commissioners, who share many of civil society's concerns, particularly regarding the aspects related to net neutrality[41].

The legislation is now in the hands of the European Parliament, who have the opportunity to amend the draft text to reflect the position of a significant, cross-party segment of the Parliament: to enshrine strong, enforceable network neutrality provisions in EU law[42].

Principles of a net neutrality law

In order to end network discrimination and ensure a thriving and neutral internet, we recommend that the following provisions are enshrined into law:

1. The internet must be kept open and neutral. Reachability between all endpoints connected to the internet, without any form of restriction, must be maintained.

2. All data traffic should be treated on an equitable basis no matter its sender, recipient, type, or content. All forms of discriminatory traffic management, such as blocking or throttling should be prohibited.

3. ISPs shall refrain from any interference with internet users' freedom to access content and use applications of their choice from any device of their choice, unless such interference is strictly necessary and proportionate to:

[38] Kroes, Neelie, The EU, safeguarding the open internet for all, 4th June 2013, SPEECH/13/498: http://europa.eu/rapid/press-release_SPEECH-13-498_en.htm.
[39] European Commission, 2012, Digital Agenda Scoreboard 2012: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/scoreboard_life_online.pdf.
[40] EDRi, 2013, Leak: Damning Analysis Of Kroes' Attack On Net Neutrality, EDRi, September 2013: http://www.edri.org/NN-negativeopinions.
[41] Reuters, 2013, EU may have to redraw telecoms plans - EU Commission official, Reuters, 2013: http://www.reuters.com/article/2013/09/09/eu-telecoms-idUSL5N0H53T320130909.
[42] See Endnote 24.

i. As a transient and exceptional measure, mitigate the consequences of congestion, while treating the same kinds of traffic in the same manner;

ii. Safeguard the integrity and safety of the network, the service, or a terminal device of the user (e.g. blocking viruses and DDOS-traffic);

iii. Block the delivery of unsolicited commercial messages (spam), but only if the subscriber has given prior consent;

iv. Respect specific legal obligations or

4. Comply with an explicit request from the subscriber, provided the subscriber may revoke the request without any increase in subscription fee at any time.

5. Use of packet inspection software (including storage and re-use of associated data) should be reviewed by national data protection regulators to assess compliance with the EU's data protection and fundamental rights framework. By default, these types of inspection techniques should only examine header information[43].

6. Complete information on reasonable traffic management practices and justifications must be accessible and foreseeable to the public. Network operators should be transparent and accountable to any changes in practices.

7. Non-neutral treatment of traffic for "voluntary" law enforcement purposes must be prohibited unless there is a legal basis and predictable procedure in the country where the restriction is being implemented. Failure to require this would be a breach of Article 52 of the Charter of Fundamental Rights and articles 8 and 10 of the European Convention on Human Rights.

Why Europe needs net neutrality legislation now

There are a variety of different approaches some states have pursued in order to uphold the principle of network neutrality; from legislative, to co-legislative, or through voluntary agreements in the private sector. Access believes that the only way to truly guarantee net neutrality in Europe is to enact strong and comprehensive legislation that clearly prevents ISPs from arbitrary discriminating online and avoids that commercial interests of major incumbent prevail on fundamental rights.

In Europe, the findings reported by BEREC prove that in the absence of a regulatory framework explicitly banning restrictions online - such as blocking and throttling - ISPs are incentivised to apply restrictions on applications and sites.

[43]OJ C 34/1, 8.2.2012, Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:034:0001:0017:EN:PDF.

For those few countries that have taken proactive steps to address this issue threatening the open and neutral internet, some countries have opted for a self-regulatory approach, such as the United Kingdom's "Open Internet code of practice", a voluntary code of conduct for ISPs to promote the offering of "full and open internet access"[44]. However, as sign-on is not mandatory, only a small number of ISPs have joined this set of commitments. It also contains loopholes: while the code specifies that specialised or restricted services shall not be labeled "internet access", it emphasises transparency (and not, for instance, banning of discriminatory practices) around any restrictions applied to cusers' internet access.

Some states have opted for a co-regulatory approach, where the legislator and the private sector co-operate. This is the case of the Norwegian Post and Telecommunication Authority (NTPA) that - in collaboration with ISPs, content providers, industry organisations and consumer protection agencies - has established the "Guidelines for Internet neutrality" - a set of principles to safeguard net neutrality[45]. However, these principles do not have any formal legal status and the Norwegian authority is not able to issue sanctions to those ISPs who do not comply with these principles.

The proposed framework is also not as robust to cover all bases of discrimination - for instance, the guidelines states that the blocking of child pornography should be considered as "reasonable traffic management". As elucidated in Access' proposed principle No. 6, that "voluntary" law enforcement purposes must be prohibited unless there is a legal basis and procedure in the country where the restriction is being implemented. Any failure to require this would be a breach of Article 52 of the Charter of Fundamental Rights.

This co-regulatory solution, while certainly providing further protections than the self-regulatory model, still does not provide the necessary guarantees that binding legislation would ensure.

Indeed, Professor Tim Wu of Columbia University - who coined the term "net neutrality" - revealed in his studies that despite the benefits offered to citizens and to both access and content providers from a neutral platform, ISPs more often favour their own services and prioritise short-term over long-term interests[46].

As evidence has shown that if businesses believe that it is not in their best interest to remain neutral, then neither self-regulation nor co-regulation will successfully persuade them to act in a manner that is thought to be contrary to their commercial interests.

[44]Open internet code of practice: Voluntary code of practice supporting access to legal services and safeguarding against negative discrimination on the open internet, 2012, United Kingdom: http://www.broadbanduk.org/wp-content/uploads/2012/08/bsg-open-internet-code-of-practice-25-jul-2012.pdf.

[45] Network neutrality, Guidelines for the Internet neutrality, 2009, Norway: http://eng.npt.no/ikbViewer/Content/109604/Guidelines%20for%20network%20neutrality.pdf

[46] Wu, Tim , 2002, Network Neutrality, Broadband Discrimination: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863

Conclusion

Network neutrality legislation will ensure that the internet remains open, democratic, and innovative throughout the European Union. Furthermore, anti-net discrimination legislation will allow the free flow of content, applications, and services, and a diversity in the types of equipment and protocols that may be used. This would effectively guarantee a level playing field for all web sites and internet technologies, to the benefit of both European citizens and all companies conducting business in the European Digital Single Market, especially startups.

Europe has long been an international policy standard-setter, especially on issues concerning human rights, and network neutrality should be no exception. Strong legislation will not only provide European citizens with the right to access an unfettered internet free from discrimination, but could also set an important standard for the preservation and promotion of the open and neutral internet around the world, benefiting users globally.

To realise and protect the full potential of the internet to enable and promote the flourishing of human rights, Europe needs a strong and comprehensive net neutrality legislation now.

References

Access, 2012, Telco Action Plan – Respecting Human Rights: Ten steps and implementation objectives for telecommunication companies.

Access, 2013, Q&A on Network discrimination in Europe.

Analysys Mason, 2012, The collapse in the value if the mobile and gigabyte: myth and reality.

BEREC, 2012, BEREC's comments on the ETNO proposal for ITU/WCIT or similar initiatives along these lines.

BEREC/European Commission, A view of traffic management and other practices resulting in restrictions to the open Internet in Europe - Findings from BEREC's and the European Commission's joint investigation, 2012, BoR (12) 30, 29th May 2012.

Chee, Foo Yun/Davenport, Claire, in: Reuters, 2013, EU may have to redraw telecoms plans - EU Commission official, Reuters.

Chilean Government, Bill 4915: Amendment to the Chilean Telecommunications Act.

Council of Europe, 2011, Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet.

EDPS, 2011, Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data.

EDRi, 2013, Leak: Damning Analysis Of Kroes' Attack On Net Neutrality, EDRi, September 2013.

European Commission, 2012, Digital Agenda Scoreboard 2012.

European Commission, 2013, Commission proposes major step forward for telecoms single market, release.

European Commission, 2013, Digital Agenda for Europe – A Europe 2020 Initiative, Digital Single Market.

European Commission, 2013, Proposal for a regulation of the European Parliament and of the Council, laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012, COM(2013) 627 final.

European Commission, Digital Agenda for Europe, Open Internet.

European Parliament, Committee on the Internal Market and Consumer Protection, 2012, Report on Completing the Digital Single Market (2012/2030(INI)), A7-034/2012, 26.10.2012.

European Parliament, Committee on the Internal Market and Consumer Protection, 2012, Report on a Digital Freedom Strategy in EU Foreign Policy (2012/2094(INI), A7-0374/2012, 15.11.2012.

Fanen, Sophian, in: Libération, 2013, Internet et applications de filtrage: une histoire de choix et de recettes, 16th January 2013.

France, Paul, Cable.co.uk, 2011, Orange partners with Spotify rival Deezer.

Gardner, David W., in: Information Week, 2009, Deutsche Telekom Restricts Skype On iPhone.

ITU: The World in 2013 - ICT Facts and Figures.

Kroes, Neelie, A Telecoms Single Market: Building a Connected Continent, 9th May 2013, SPEECH/13/622.

Kroes, Neelie, The EU, safeguarding the open internet for all, 4th June 2013, SPEECH/13/498.

Kroes, Neelie, The politics of the completing the telecoms single market, 30th May 2013, SPEECH/13/484.

Meyer, David, Gigaom, 2013, Deutsche Telekom's "anti-net-neutrality" plans alarm German government.

Network neutrality, Guidelines for the Internet neutrality, 2009, Norway.

OECD, 2005, Input to the United Nations Working Group on Internet Governance (WGIG).

OJ C 34/1, 8.2.2012, Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data.

Omanovic Edin, Blog on: Privacy International, 2012, The Kremlin's new Internet surveillance plan goes live today.

Open Letter by European CEOs to the European Commission.

Open Rights Group, 2013, quick guide to Cameron's default Internet filters.

Open internet code of practice: Voluntary code of practice supporting access to legal services and safeguarding against negative discrimination on the open internet, 2012, United Kingdom.

Plum Consulting, 2011, The open internet – a platform for growth – A report for the BBC, Blinkbox, Channel 4, Skype and Yahoo: London, p. 19.

Radio Bruxelles Libera, 2013, Article in English on the Slovenian law on net neutrality, 3rd January 2013.

Royal Pingdom, 2012, Infographic.

Schaake, Marietje, 2013, Guaranteeing competition and the open internet in Europe.

Jackson, Nicholas, in: The Atlantic 2011, United Nations Declares Internet Access a Basic Human Right.

The Web Foundation, The Web Index 2012.

Tiki-Toki, EDRi's timeline.

UN General Assembly, 17th Session, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, No. 27 (A/HRC/17/27), Official Record, Geneva, 2011.Network neutrality, Guidelines for the Internet neutrality, Norway, 2009

Van Dalen, Ot, Bits of Freedom, Summary from Bits of Freedom of the amended Dutch Telecommunications Act.

World Bank Group, Summary of the 2009 World Bank Group Report.

Wu, Tim, 2002, Network Neutrality, Broadband Discrimination.

Network Neutrality under the Lens of Risk Management

by Alejandro Pisanty

I propose to analyze the problem of Network Neutrality under the lens of risk management, *i.e.* to apply basic disciplines of risk management to the formulation and to possible violations of the principle of Network Neutrality (NN.) This perspective is productive in giving the violations a treatment that can be commensurate with their likelihood and impact as well as with the cost of their avoidance, mitigation, and remediation.

The components of risk management considered in this paper have been compounded from widely-used frameworks (Landoll, 2011; Miller, 1992; Oren, n/d). Impact and likelihood are approximate and together with naming and defining the risk are part of risk identification. Avoidance and prevention are listed separately; avoidance assumes that violations to Network Neutrality exist, whereas prevention is action intended to cause the impede or forestall Network Neutrality violations.

The conceptual framework for the analysis is as follows:

Network Neutrality is the principle – or extension of a more fundamental set of principles, among which the end-to-end principle (Van Schewick, 2010) stands out – by which an Internet access provider (ISP) delivers Internet Protocol (IP) traffic to its users without discrimination of port numbers, protocols, origin, destination of contents of the communication carried by the IP packets. Common expressions of this principle include the expression "the five alls" meaning all ports, all protocols, all origins, all destinations, all contents are carried in a non-discriminatory fashion, which we use in communications by the Internet Society of Mexico and some of our teachng. The canonical reference for definitions of Network Neutrality is Wu (2003); further updates and discussion are available on Wu (n/d) and OFCOM (2011).

Several constraints apply to the above statement defining Network Neutrality for the purposes of this paper:

First, in actual practice it is impossible to comply with the "five alls" due to operational considerations. ISPs may need to block some ports and origins, in particular, due to Best Practice (or, in organizations like the IETF, Best Current Practice, BCP) recommendations (such as blocking port 25 to avoid the use of open relays for e-mail spam), traffic engineering and traffic shaping in order to provide acceptable service in the face of varying network conditions, response to attacks among which Distributed Denial of Service attacks (DDoS) are prominent, congestion, and other needs of network and service management. ISPs may also be forced to block some traffic for legal reasons, such as a prohibition, within a given country

or territory, of providing certain contents (hate, racial or gender discrimination, child-abuse imagery, etc.)

Filtering and blocking may be operated by a wide variety of technical means. Among the simplest and most common are ACLs (Access Control Lists) in routers and switches, which filter out IP addresses or address blocks. Other simple filtering and blocking techniques are based on domain names, which in some cases has been attempted by tampering with the Domain Name System (DNS) close to the network core, with deleterious effects already described by Crocker *et al.* (2011).

Filtering, blocking and throttling are also known to be performed on the basis of Deep Packet Inspection (DPI), which allows the ISP or other operator to obtain information about the contents and other characteristics of the communication beyond the information contained in the IP packet headers. DPI is considered in itself a violation to the end-to-end principle to some extent. We will not enter the extensive discussion about this subject and consider it as a violation, or tool for Network Neutrality violations, when its use fits the definitions in this paper.

Taking these factors into account allows for a sharper definition of Network Neutrality, in particular by focusing on "discrimination." The most widely accepted definitions of Network Neutrality leave room for some actions to be considered non-violations even though they do not deliver the "five alls".

Allowance is thus made for legally-mandated blocking and filtering, as well as for filtering, blocking or throttling traffic for traffic engineering purposes. Traffic engineering is intended to optimize the operation of a network and to respond to contingencies; what it does not allow for is performing any of these actions selectively in order to favor some traffic over another for commercial reasons such as can appear when an ISP is vertically integrated or otherwise allied with a content provider, and the ISP in this case selectively eases the traffic from this provider against some or all others.

It is also generally accepted that if an ISP or similar provider is to incur in any of the above practices without violating Network Neutrality, the action should be in so far as possible legally motivated, temporary, and communicated to the user in a clear way (the transparency requirement.)

There are also additional, important variations in these concepts depending on country and approach, particularly depending on whether the approach is market and competition oriented, regulatory, or legislative. At the time of this writing most countries have decided not to enact legislation mandating Network Neutrality and have not included it in the telecommunications regulations, so are mostly watching the situation evolve and allowing competition in open markets as a way to ensure that ISPs will provide access to "all fives" except within the allowances already described. A few countries, such as the Netherlands and Chile, have laws mandating Network Neutrality, and they merit watching more closely for lessons learned.

Further precisions to the definition and our analysis in this paper refer to the provider involved; ISPs are but one widely accepted category and well-defined in national legislations, but variations may exist for differences in legislation or language or due to market structures.

We have designed our framework for managing violations to Network Neutrality as risk in a way that allows for broad variations within the uncertainty of the definition of Network Neutrality and of the party potentially incurring in such violations. The risk management framework is designed to be robust against differences in definition over geography and time.

The subject of the violations is constructed as a broadly defined persona. Again, broad definitions are chosen in order to provide a robust framework.

The persona around which the framework is designed is mainly an individual Internet user who uses the Internet for access to information; interpersonal communication through e-mail, instant messaging and other text, sound and video, whether synchronous or asynchronous, one-to-one, one-to-many or many-to-many; interactions with and through online social networks, fora and communities; peer-to-peer, client-server, or otherwise; publish content online through social media, blogs, newspapers, online fora, scientific and academic publications, video and audio websites and portals, augmented- and virtual-reality spaces and others; purchase and sell physical and electronic goods and services; and many other activities as listed in surveys such as those performed by the Pew Trust in the US and INEGI and AMIPCI in Mexico.

In so far as possible, the persona definition is neutral and robust for differences in gender, nationality, place of residence, socio-economic status, age, and other demographic variables unless otherwise noted. Particular attention is paid to non-commercial use of the Internet by the persona. However it is also assumed that the user represented in the persona may be making commercial use as a buyer of goods and services, and a seller at least of personal services such as an employee, independent professional, or occasional seller. A different analysis applies for the enterprise, and it requires a different persona which may be studied later.

For the purposes of the framework, both wired and wireless communications are considered. Participants in the Network Neutrality debate in some jurisdictions make or try to make a strong distinction between both. This is due especially to the much stronger constraints that wireless communications face in provisioning bandwidth, throughput, tolerable latency and jitter, and their basic inputs such as spectrum allocations and antenna/cell locations.

The way to reconcile these two sets of constraints for the framework is to judge the reasonableness of operators' actions in each at given times. Special conditions may mitigate a harsh judgment of Network Neutrality violations for wireless operators if they face temporary congestion of their networks. These conditions may include network congestion, damages to the networks' links or active equipment, and other deliberate or accidental attacks, and may appear in natural disasters, violent social events, and non-violent but highly-attended or widely communicated social events.

For this framework we are not making separate analysis for intentional and non-intentional violations. The usual distinctions of political, financial, etc. types of risk are agglomerated for simplicity. The actions suggested have been designed or selected, and ranked, so that risk management is kept aligned and proportional.

Our main scenario therefore is one in which we seek to establish possible responses to deliberate violations of Network Neutrality due to commercial interest, and allow as well to some degree of politically generated filtering and blocking.

Violations to Network Neutrality

Table 1 summarizes the approach. It is based on the consumer's point of view. A new table must be written for each stakeholder or a color or graphic tool must be introduced to signal the different risk valuations and strategies that apply.

Entries in the table indicate the actions the user should consider to perform according to the risk described in the line in which the cell is found, and for the risk-management action indicated in the column. When more than one action is listed, the order in the list is the order of escalation suggested. For example, a user who finds that a certain port is closed by her ISP should first complain to the ISP and request for the port to be opened; if this does not produce the desired effect, or an explanation why the ISP will not open the port, the user should bring a formal complaint to the appropriate authority (telecommunications regulator, competition authority, consumer defense authority or organization, etc.) Should this in turn fail, one option for the user is to create pressure on the ISP through a public outcry, maybe using social media for the purpose. The order of escalation should be clear in this example.

Another table of interest would perform and summarize the analysis for a provider of services over the Internet (OSP) which could be affected by violations to NN by an ISP or carrier on which the OSP relies, either by contract or as an unavoidable intermediary in the Internet interconnection ecosystem.

The individual user's concerns with Network Neutrality revolve around the fulfillment of the principle's "five alls" – unfettered access to all protocols, all ports, all contents, all origins, all destinations of Internet communications, barring well-defined and limited exceptions for traffic management and security.

Thus the individual user's concerns are affected when an ISP limits or diminishes access in ways that to which the user is sensitive. Not being able to access some ports, protocols, etc. hampers the Internet user experience and may infringe consumer or citizen rights, thus spanning a spectrum that goes from the technical through the commercial and potentially all the way to the political.

The general Internet user may face Network Neutrality violations with but limited tools to detect them, to pinpoint which they are, to react to them, and in other ways to prevent and avoid them. It is in the interest of global stewardship of the Internet, therefore, that Network Neutrality violations be easily detected, and that users have ways to deal with them. Further, in contrast to other stakeholders, design for users must be based on the assumption that the

user has frugal – at best – economic resources, very limited technical knowledge, extremely limited technical tools, and near-nil political clout at the individual level (and in most countries and conditions, nil collective power as well.)

The OSP's concerns are ability to reach all users, ability to reach all clients, the quality of user experience and the factors this in turn is measured by, and unfettered access to and through infrastructures such as CDNs which may form complex layers between the OSP, its users and its clients.

The OSP's actions will differ from an individual user's in some significant aspects. The OSP may be able to negotiate directly with an ISP or carrier, or lobby a regulatory agency or even a legislature where the individual user can't, for example, given the power that is granted on the OSP due to its corporate nature and economic value *vis á vis* the limited power of an individual consumer – further, in a foreign jurisdiction.

The individual user's and the OSP's interests – and therefore to some extent risks – may become aligned in cases such as that in which the user's interest is to access and use the OSP's services and these are blocked, throttled, or in some other way affected negatively by Network Neutrality violations by intermediaries.

Risk sharing or risk transfer has not been considered in the table. The possibilities of transferring violations of Network Neutrality to third parties in a meaningful way or of spreading the risk through sharing have been considered to make little or no sense at this stage and therefore excluded from the study for now.

Risk name	Impact and Probability	Avoidance	Detection	Mitigation	Response	Contingency plan	Continuity	Prevention
Blocking of: Port Protocol Source Destination Traffic pattern Content by DPI	P high I high	VPN unless blocked by ISP as well	Netalyzr Crowdsourcing Verification with sender or other third parties	VPN IP address spoofing Identity masking	Complaint Public complaint Public outrage campaign Lawsuit if laws broken	VPN Site provisioned by alternate ISP	Public advice Change supplier Redundant provisioning Lobby/pressure ISP or other infringing party Lobby/pressure parties which can force change of ISP conduct, such as consumer authorities and telecommuni	Consumer regulation Market and competition regulation Telecoms law NN law Strong consumer and citizen voice

							cations, market and/or competition regulators	
Throttling for Own Client/Ally Political Other vertical Mislabeling	P high I variable	Hard (VPN may not cause significant relief)	Speed of downloads; connection-dependent process stability (eg SSH); Large samples needed	CDN run by OSP; cache or proxy; alternate unthrottled source (possibly P2P upload)	Complaint Public complaint Call for regulatory intervention Public outrage (harder than for blocking) Litigation	CDN Site provisioned by alternate ISP Patience	Patience	Consumer regulation Market and competition regulation Telecoms law NNlaw Strong consumer and citizen voice
Traffic Management	P extremely high I variable	If within accepted rules, no action needed	ISP notices Netalyzr Crowdsourcing	If within accepted rules, no action needed, otherwise go to next line in table	If within accepted rules, no action needed, otherwise go to next line in table	If within accepted rules, no action needed, otherwise go to next line in table	If within accepted rules, no action needed, otherwise go to next line in table	If within accepted rules, no action needed, otherwise go to next line in table
Failure to communicate to users Absence of advice Misleading advice Temporary measures made permanent		Double ISPs (assuming no collusion)	Verify with third parties News Social media Crowdsourcing	Create own warning and circulate; make viral through social media	Create own warning and circulate; make viral through social media Lobby/pressure ISP and parties with power over its conduct	Create own warning and circulate; make viral through social media Lobby/pressure ISP and parties with power over its conduct	Create own warning and circulate; make viral through social media Lobby/pressure ISP and parties with power over its conduct	Change supplier if market and rules allow Call on regulators for telecommunications, competition, consumer rights

P= probability or likelihood

I = impact

Notes to the table:

1. VPN means "virtual private network." It is potentially useful to circumvent Network Neutrality violations by not obscuring to the ISP the IP address, domain name, or other revealing characteristics of the website, email destination, etc. with which the user communicates.
2. "Netalyzr" is software from the University of California at Berkeley which allows users to identify a large set of features of Internet connections, including proxies they have not set, inaccessible ports, IP addresses, and other potential Network Neutrality violations. It is used in this paper to represent both the specific Netalyzr software and any other user-operated software tools that allow users to detect whether some ports, protocols, communication origins, destinations or contents are not accessible to them. The use of these tools is more effective and credible after proper training and may need considerable sampling for definitive results. For example, Netalyzr lights an alarm when IP address and domain name do not match "whois" records; this may be due to supplantation, man-in-the-middle (MITM) attacks, Network Neutrality violations, or decisions by the portal owner to use a CDN. This last situation is not uncommon for large media, online services, and OSPs. The user must interpret the results with great care.
3. The detection of throttling may be much more difficult than the detection of outright blocking. Numerous measurements with quality tools, with a good sampling design, may be needed in order to prove it definitively. In throttling the ISP may use a large variety of techniques to diminish the speed at which certain selected communications operate. The user may perceive throttling through slow downloads, broken connections due to timeouts, pixelization and freezing in images and video, and related phenomena. These events are also usual in some underprovisioned or congested networks, may be occasional even when not deliberate, and therefore may be attributed to uncertain causes. Therefore, the infringing ISP may deflect complaints and criticism by placing the cause of the events on the user's side or on the vagaries of the best-effort approach of Internet communications embedded in the protocols and design.
4. Unless the user has a strong service-level agreement (SLA) with the ISP, a number of complaints may be dismissed as mentioned for throttling. Strong SLAs usually contain definitions, expected levels of availability, upper bounds on "ping" times, delay, and jitter in communications, as well as penalties for violations. They are not common for individual Internet users (home or small-business contracts.) When they are available they are costly and mostly oriented to business contracts. This paragraph covers "response."
5. Impact and probability must be determined for each risk and in each different set of conditions (time, place, stakeholders, intended or actual action.) The impact of ISP actions on Network Neutrality is deemed high if the actions are liable or proven to seriously hamper the user´s ability to communicate, and low if the opposite is the case or if avoidance and mitigation are readily available. The probability for each risk is assessed on grounds of history. Thus, for example, port blocking to impede access to

VoIP is assessed a high probability because it has reported in numerous occasions in several different countries.

To further facilitate use of the table an example is provided:

Assume that a port or set of ports are being blocked by an ISP, corporate part or ally of a telephony company, in order to impede the use of an application such as VoIP (voice over IP) or IP telephony. This could be done by the company in order to preserve its source of income in conventional telephony against the competition of the much cheaper or free VoIP service. The user's conduct following the table would start in row 1 of the table.

a. The user's first need is to establish with reasonable certainty that the port blocking condition is indeed in operation. To detect this she can:
    i. Use the same equipment in a different network and find that in this new one the service is not blocked.
    ii. Connect to a VPN and find that using the VPN the service is not blocked. This assumes that the VPN is not blocked by the ISP and that the service is not blocked by the VPN.
    iii. Run software such as Netalyzr which will tell the user whether some port numbers or ranges are found blocked, and provide some other diagnostics which could also be useful to dissect the situation.
b. Once the user has certainty that the ISP is violating Network Neutrality by blocking port numbers she can:
    i. Call the ISP and find out whether this is a deliberate condition or an accidental one.
    ii. In case it is accidental the user can have the condition lifted by the ISP.
    iii. In case that the port blocking is intentional the user can request its lifting, starting through customer service and its escalation.
c. Should the above steps fail the user may have one course of action left which is to go public with her complaint, starting with social media, consumer associations, consumer authorities, telecommunications regulators, competition authorities, and media and social media campaigns. The specifics of each case will be determined among other factors by the applicable legislation, whether the legislation is enforced, etc.
d.
e. Mitigation. The user may find a work-around to get to the contents or services being blocked, by using a VPN or an alternate ISP. This in turn may require changing physical location, to an Internet café, academic facility, or other that doesn't suffer from the port blocking.
f. Contingency plan. The user need be prepared to detect the port blocking and enact the mitigation actions immediately, for which access to a VPN must have been obtained in advance (*e.g.* generating an account, paying for it, and testing regularly that it is available and fulfills the purpose.)

g. Continuity plan. The user continuity plan will be a combination of the countermeasures already listed, and will be deprecated once regular access conditions have been reestablished.
h. Prevention. Preventive measures against port blocking directed to impede access to defined services requires inducing change in the ISP's behavior. In order the measures are complaints and protests directly to the ISP, public campaigns that force the ISP to change, or the enactment of regulatory or legislative measures. This succession matches well the history of Network Neutrality legislation In the Netherlands.

References

Crocker, S., Dagon, D., Kaminsky, D., McPherson, D., & Vixie, P. (May 2011). *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill,* retrieved from http://www.shinkuro.com/PROTECT%20IP%20Technical%20Whitepaper%20Final.pdf

ISACA (2011). *The RiskIT Framework.* Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/RiskIT_FW_30June2010_Research.pdf

Landoll, D.J. (2011). *The Security Risk Assessment Handbook, 2nd. Ed.*, Boca Raton, FL, USA: CRC Press

Miller, K.D. (1992). A Framework for Integrated Risk Management in International Business. *J. Int. Bus. Stud 23*, 311-331 online at http://www.jstor.org /stable/154903

OFCOM (2011). *OFCOM's approach to net neutrality,* http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/statement/statement.pdf version of Nov. 24 2011

Oren, S., 2001. Market Based Risk Mitigation: Risk Management vs. Risk Avoidance, retrieved from http://www.pserc.wisc.edu/ecow/get/publicatio/2001public/marketbasdriskmitigation-v2-oren.pdf

Van Schewick, B. (2010). *Internet Architecture and Innovation,* Cambridge, MA, USA: MIT Press

Wu, T. (n/d). http://timwu.org/network_neutrality.html

Wu, T. (2003). *Network Neutrality, Broadband Discrimination* Journal of Telecommunications and High Technology Law, Vol. 2, p. 141, online as http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863

Net neutrality and Quality of Service

by Louis Pouzin

Foreword

The terminology "Net Neutrality" associates two words for which there is no precise definition. Thus we must define here the meanings we use in the body of the present document.

"Net" is an abbreviation for Internet. But what is Internet ? Initially, in 1973, the term became used as a short for internetwork, that is a set of interconnected packet switching networks. The term "catenet" was proposed [1,2] for this level of communication infrastrucure. Actually over the years people kept using the word internet to mean any and everything (hardware, software, applications, services) including catenet itself. Thus the meaning of the word "internet" became a hodgepodge of fuzzy interpretations and misconceptions making unlikely any public rational consensus on desirable policies and improvements.

In this document, "net" means "catenet".

Neutrality is often understood as non partisan, when bringing up several viewpoints or proposing various alternatives to a disputed resolution. This is a human or institutional posture. When associated with (computer) network it is literally meaningless. Nevertheless people somehow invent their own interpretation of network neutrality fitting their concerns. Usually their perception derives from a feeling of being unfairly discriminated in ways they get network service. At the same time they cannot advance technical specifications intended to make the network neutral.

Implementation of the net neutrality principle

The immediate question is: what is the principle ?

Many people think that all packets should be handled equally. E.g. packets sent to a high bandwidth destination would be delayed so that they would not exceed the number of packets sent to a low bandwidh destination. Or packets carrying voice conversation would have to wait for an available slot in a common output queue. Etc.

A quick scan for "network neutrality" in a search engine turns up scores of references, e.g. [3], based on various usage assumptions and network characteristics.

It is clear that interpretations vary with net operators, content providers, and end users.

An example is a set of principles worked out in Norway [9] in 2009. For a time this was hailed as a model of a broadly agreed consensus. However, in 2012 this agreement fell apart [10], due to a major increase in bandwidth requirements for video traffic.

Net operators

Net operators endeavor to handle data within the technical constraints of the service expected by end users, e.g. interactive session, transaction, file transfer, voice conversation, web page, voice or video streaming, real time. Each type of service usually expects a minimum transit delay, or a minimum bandwidth, or a stable delivery rate. Fulfilling all these constraints at any time cannot be achieved without monitoring data flows and moving packets within specific time frames. In case of bandwidth shortage some arbitration is needed among flows so that the service degradation perceived by users remain tolerable. Obviously there is no magic recipe to guarantee that all users perceive an equal degree of degradation.

When bandwidth shortage is severe it may be necessary to delay some high bandwidth flows which reduce low bandwidth ones to a trickle. That is, some types of less demanding users get priority. This is service management.

Typically from their source to end users data flows are carried through more than one operator. Nets are usually independent systems applying their own service management policy. Thefore one should not expect a natural built-in consistency among all operators. Mutual adjustments result from experience, proper selection of net partners, and administrators preferences.

Content providers

A content provider could be, for example, a heat sensor, a camera, a PC or a data center, that is, any computing system collecting or serving data, but not a packet carrier. They are connected to one or more nets and are used remotely in interactive, transaction or streaming mode or file transfer. As long as their traffic flow is substantially lower than the net capacity there is no specific issue to be raised. On the other hand providers may not receive data in time, or they may exhaust the net capacity.

Net overload or insufficient data collection frequency may cause provider's data loss, which might be mitigated with buffering (storage) and compression, if applicable by providers. Statistics collection is presumably more tolerant to some minimal data loss. Alarms are not.

Massive provider data transfer is more likely to trigger congestion in a part of the net. This is unwelcome by net operators, and a major bone of contention with content providers. This is not a matter of technical arguments. The crux of the matter is money: who should pay for increasing net capacity. Is more capacity really justified, when more than half a web page is preempted by unwanted publicity and visual gadgets ? Why is the provider not applying better data compression ?

End users

A dominant majority of end users are not (interested in becoming) net experts. They pay their ISP, and other providers, for various services, net access, search engines, email, social nets, banking, travel services, phone, music, TV, etc. They feel ripped off when the service is slow, broken, or error 404 *(typical diagnostic for a missing page).* There could be a number of

reasons for the degradation, ISP or net adapter, some operator trouble, a slow application server, a bugged DNS, a clumsy routing through the net, a virus, or other. For the user it's the "internet". After several calls to support, and much wasted time, he blames the net operator, which has a reputation of favoring some profitable clients, to the detriment of his kind of user. Adding to the picture a one-sided contract whereby the user is under threat of being cut off the net while the operator or ISP is immune from complaints. In conclusion the net is not neutral, not to say crooked.

Conflict generators

Users reactions may be partially subjective, but quite predictable. As ISP/operator contracts are one-sided, and exclude any quality of service evaluation, users may think they pay for other users enjoying better service, and it's certainly true in some areas of the net. Without factual observation of the service characteristics there cannot be any credible assertion of neutrality. The result is an endemic user suspicion and frustration. Nevertheless the net neutrality they call for may be just a mirage.

Quality of service (QoS)

Initial QoS definition for telecommunications was produced by ITU in 1994. Its definition for computer networks was more arduous due to environment complexity, which keeps growing. An overview is in Wikipedia [4]. Selected research articles have elaborated solutions applicable to the net [5,6,7]. Hence best effort, meaning no QoS, is no longer the essence of the net. End-to-end flow characteristics are now predictable.

A significant result is a new business model for the net. An operator or ISP is in a position to offer users differentiated classes of guaranteed service. In return a user is in a position of checking that he gets what he pays for, or claiming a compensation. What other users are getting becomes immaterial. Each user pays for his own QoS. Net neutrality no longer makes sense in the net context. Users may resent the same QoS being charged at lower fees to some clients, and complain about unfair competition, but this would be a strictly commercial dispute unrelated to the net operation.

As it occurs, QoS may not be implemented properly. Some net or ISP may enforce filtering based on content technical characteristics. E.g. it is reasonable to defer the delivery of huge attachments to a low bandwidth device. Thus users need well documented information on conditions which could interfere with QoS. Options should be available to let users arbitrate between options, e.g. cutting video or images to speed up delivery.

Who is charged for QoS ? Even though the subject appears more commercial than technical, it may have a strong influence on traffic. Some content providers can flood the net, in clogging all service classes. Unless a minimum QoS is maintained in each class some users could be denied service. That is, traffic thresholds may be needed to limit production or consumption during peak times (similar to electricity). Content providers and users contribute to net load, and should be charged to facilitate traffic smoothing.

Closed internet

There are more factors that may distort service. E.g. a file transfer class may be limited to very short files, a video channel may reduce image resolution, etc. Such constraints may not be attractive for users, but on a competitive market they could hopefully find better providers.

Presently accessing internet services requires either an IP address or a a domain name. Web applications are often designed only for domain names. These names are registered in the DNS, a directory managed by a private company (Verisign) under contract with ICANN, a private monopoly imposed by the US gov without any international legitimacy. Domain name rental fees paid by users crawl up the food chain to ICANN through retailers (registrars) and Verisign.

Apart from this cash cow scheme there is a neutrality issue. Like any monopoly ICANN protects its turf against competition: its DNS contains only names paying a rental fee. There are non-ICANN DNS [8] containing more domain names that are not in the ICANN DNS. However, ISPs, browsers and mailers on the market know only the ICANN DNS. This may be fixed, but needs a user's initiative, a common deterrent.

Another case observed in some hotels and institutions is denial of net access when the user device has been equipped with non ICANN DNS addresses. This is rather surprising since other institutions have no need to protect the ICANN monopoly nor the NSA tracking.

Being under US gov proclaimed jurisdiction, the ICANN DNS content is monitored, if not altered, out of users knowledge. Personal and confidential information can be collected when the root servers are used. Hence some users have solid reasons for not using the ICANN DNS.

Anyhow, denying users their choice of DNS is an attempt to privacy, and an abuse of dominant position.

Conclusions

The best effort internet service shows its age (1983). QoS is sorely needed for critical applications. However upgrading the present infrastructure appears doomed to a fate similar to IPv4 - IPv6 upgrading. Actually class 0 of QoS is what we have, et what many people are satisfied with. Why not start building a new infrastructure ?

References

1 - Pouzin L. - Interconnection of packet switching networks, INWG note 42, Oct. 1973. http://bärwolff.de/public/Pouzin-1973-Interconnection-of-Packet-Switching-Networks--INWG-Note-42.pdf

2 - Pouzin L. - A proposal for interconnecting packet switching networks. EUROCOMP, Brunel Univ., May 1974, 1023-1036.
The Auerbach Annual - 1975 Best computer papers. 105-117. Isaac Auerbach ed.

3 - http://www.ocf.berkeley.edu/~raylin/whatisnetneutrality.htm

4 - http://en.wikipedia.org/wiki/Quality_of_service

5 - R. Boutaba, N. Limam and J. Xiao. Autonomic Principles for Service Management: Performance, Fairness and Stability. In Proc. of the 2nd International Symposium on IT Convergence Engineering (ISITCE). Pohang (Korea), 19-20 August, 2010.

6 - Issam Aib and Raouf Boutaba - Business-driven optimization of policy-based management solutions, in: 10th IFIP/IEEE International Symposium on Integrated Network Management (IM 2007), Munich, Germany, 2007.

7 - Jin Xiao, R. Boutaba - QoS-aware service composition and adaptation in autonomic communication - Journal on Selected Areas in Communications, IEEE (Volume:23, Issue: 12) pp. 2344-2360, Dec. 2005.

8 - http://en.wikipedia.org/wiki/Alternative_DNS_root

9 – Norway gets net neutrality—voluntary, but broadly supported
http://arstechnica.com/tech-policy/2009/02/norway-gets-voluntary-net-neutrality/

10 - Norway ISP Ends Net Neutrality Support
http://news.heartland.org/newspaper-article/norway-isp-ends-net-neutrality-support

Net Neutrality:
Past Policy, Present Proposals, Future Regulation?

by Christopher T. Marsden

Introduction

Network neutrality is a growing policy controversy. Traffic management techniques affect not only high-speed, high-money content, but by extension all other content too. Internet regulators and users may tolerate much more discrimination in the interests of innovation. For instance, in the absence of regulatory oversight, ISPs could use Deep Packet Inspection (DPI) to block some content altogether, if they decide it is not to the benefit of ISPs, copyright holders, parents or the government. ISP blocking is currently widespread in controlling spam email, and in some countries in blocking sexually graphic illegal images. In 1999 this led to scrutiny of foreclosure of Instant Messaging and video and cable-telephony horizontal merger[1]. Fourteen years later, there were in 2013 net neutrality laws implemented in Slovenia, the Netherlands, Chile and Finland, regulation in the United States and Canada[2], co-regulation in Norway, and self-regulation in Japan, the United Kingdom and many other European countries[3]. Both Germany and France in mid-2013 debated new net neutrality legislation, and the European Commission announced on 11 September 2013 that it would aim to introduce legislation in early 2014. This paper analyses these legal developments, and in particular the difficulty in assessing reasonable traffic management and 'specialized' (i.e. unregulated) faster services in both EU and US law. It also assesses net neutrality law against the international legal norms for user privacy and freedom of expression.

Policy Debate Regarding Traffic Management

Network neutrality[4] is the latest phase of an eternal argument over control of communications media. The internet was held out by early legal and technical analysts to be special, due to its

1 See Lemley, MA and Lessig, L. (2000) *The End of the end-to-end: preserving the architecture of the internet in the broadband era*, UC Berkeley Public Law Research Paper No 37. See further Marsden, C. (1999) Council of Europe MM-S-PL(1999)012: '*Pluralism in the multi-channel market. Suggestions for regulatory scrutiny'*, at S.5.1: http://www.coe.int/t/dghl/standardsetting/media/Doc/MM-S-PL(1999)012_en.asp

2 Candeub, Adam and McCartney, Daniel John (2012) *Law and the Open Internet*, 64 Federal Communications Law Journal 3, pp.493-548, Available at SSRN: http://ssrn.com/abstract=1943747; CRTC (2009) *Review of the Internet Traffic Management Practices of Internet Service Providers*, at http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm

3See Marsden, C. (2013)*Network Neutrality: A Research Guide* Chapter 16 in 'Handbook Of Internet Research', I. Brown, ed., Edward Elgar, at SSRN: http://ssrn.com/abstract=1853648

4See Marsden, C, 'Network Neutrality: A Research Guide' in Brown, Ian (ed) *Handbook Of Internet Research*' (Cheltenham: Edward Elgar, 2013).

decentred construction,[5] separating it from earlier 'technologies of freedom' including radio and the telegraph.

Dividing net neutrality into its forward-looking positive (or 'heavy' and backward-degrading negative (or 'lite') elements is the first step in unpacking the term, in comprehending that there are two types of problem: charging more for more, and charging the same for less[6]. Abusive discrimination in access to networks is usually characterized in telecoms as a monopoly problem, manifested where one or two ISPs have dominance, typically in the last mile of access for end-users. ISPs can discriminate against all content or against the particular content that they compete with when they are vertically integrated. Conventional US economic arguments have always been broadly negative to the concept of net neutrality, preferring the introduction of tariff-based congestion pricing.[7] Hahn and Wallsten explain that net neutrality[8] 'usually means that broadband service providers charge consumers only once for Internet access, don't favor one content provider over another, and don't charge content providers for sending information over broadband lines to end users.'

Development of European legal implementation of the network neutrality principles has been slow, with the European Commission referring much of the detailed work to the new Body of European Regulators of Electronic Communications (BEREC), which developed an extensive work programme on net neutrality in 2011-12[9]. At European Member State level, statements of principle in favour of net neutrality have been made in for instance France, but no legislation was implemented by mid-2013,[10] though Netherlands and Slovenian laws had been passed in 2012 and awaited implementation in mid-2013.

I now briefly summarize the debate to date.

---

5 The 'Internet' is a network of Autonomous Systems, of which about 40,000 are of a scale that is relevant. See Haddadi, Hamed et al (2009) Analysis of the Internet's structural evolution, Technical Report Number 756 Computer Laboratory UCAM-CL-TR-756 ISSN 1476-2986.

6I have argued that the real problem lies in the 'middle mile' of interconnection, in Marsden, C, *Network Neutrality: Towards a Co-regulatory Solution*, (London: Bloomsbury Academic, 2010).

7See David, Paul (2001) 'The Evolving Accidental Information Super-Highway', 17(2) Oxford Review of Economic Policy pp159–187.

8Hahn, Robert and Scott Wallsten, (2006) 'The Economics of Net Neutrality' AEI Brookings Joint Center for Regulatory Studies: Washington, DC at <www.aei-brookings.org/publications/abstract.php?pid=1067>.

9See generally http://berec.europa.eu/eng/about_berec/working_groups/net_neutrality_expert_working_group_/282-net-neutrality-expert-working-group

10Cave, M, DAF/COMP/WP2(2011)4 Directorate For Financial And Enterprise Affairs: Competition Committee Working Party No 2 On Competition And Regulation: Hearing On Network Neutrality Paper by Mr. Martin Cave (2011).

Network Neutrality Regulation in the US

While issues about potential discrimination by ISPs have been current since at least 1999, the term 'network (net) neutrality' was coined by Tim Wu in 2003.[11] In the period since, the debate was dismissed as 'an American problem due to abandonment of network unbundling' and common carriage. Competition in the US is 'inter-modal' between cable and telecoms, not 'intra-modal' between different telecoms companies using the incumbents' exchanges to access the 'Last Mile'.[12] Instead of regulated access to both cable and telecoms networks, there are now less regulated 'information' not 'telecommunications' services.

FCC Chair Michael Powell declared: 'I challenge the broadband network industry to preserve the following Internet Freedoms: Freedom to Access Content; Freedom to Use Applications; Freedom to Attach Personal Devices; Freedom to Obtain Service Plan Information.'[13] The 'Four Freedoms' were applied in the Internet Policy Statement,[14] *Madison River*[15], the AT&T and Verizon mergers, and the *Comcast* action. Madison River was an easy case: the abuse was incontrovertible and defended as a legitimate business practice, the vertical integration of the ISP with its voice telephone service meant it had obvious incentives to block its competitor, and the practice was intended to degrade its customers' internet access. It was an example of negative network neutrality: customers signed up for broadband service with the ISP, but it chose to degrade that service in the interest of preserving its monopoly in telephone service. Madison River is a small consumer ISP, not a large behemoth national carrier. The merger of AT&T and BellSouth undertook various commitments not to block other companies' applications directed to their users.[16] FCC then made a 2008 Order against Comcast, a major cable broadband ISP.[17] Comcast deposition to the FCC stated that it began throttling P2P filesharing application BitTorrent in May 2005–2006, slowed by use of Sandvine technology. The FCC ruling was against Comcast's attempts to stop P2P by sending phantom RST reset packets to customers reflects another 'easy' case, that is about as "smoking gun" as the VOIP blocking in *Madison River* in 2005[18]

American Recovery and Reinvestment Act 2009, included a broadband open access stimulus:[19] on extending broadband into under-served areas, with open access and net

11Wu, T (2003) 'Network Neutrality, broadband discrimination', 2 Journal on Telecommunications and High-Tech Law 141.

12Communications Act of 1934 as amended by Communications (Deregulatory) Act of 1996, 47 USC.

13Powell (2004) Four Freedoms speech, at <http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-243556A1.pdf>.

14FCC (2005) Internet Policy Statement 05-151.

15FCC (2005) *Madison River Communications, LLC*, Order, DA 05-543, 20 FCC Rcd 4295

16FCC (2007) *In AT&T Inc and BellSouth Corp* Application for Transfer of Control, 22 FCC Rcd 5562.

17FCC (2008) Memorandum Opinion and Order, 23 FCC Rcd 13028 ('ComcastOrder').

18See Karpinski, R, Comcast's Congestion Catch22, 23 January 2009, at <http://telephonyonline.com/residential_services/news/comcast-congestion-0123/index1.html>

19American Recovery and Reinvestment Act 2009, at Division B, Title VII, Section 6001(k)2, A, D, E.

neutrality provisions built into the grants.[20] FCC then made an Order of 23 December 2010,[21] challenged before the courts in 2012-13. FCC in 2011-13 refused several times to intervene in interconnection and piering disputes that were claimed by CDNs to unreasonably impair traffic contrary to the controversial and *sub judice* net neutrality rules[22]. Implementation of the technical means for measuring reasonable traffic management are tested in a self-regulatory forum, the Broadband Industry Technical Advisory Group (BITAG). Its specific duties include that to offer 'safe harbor' opinions on traffic management practices by parties making formal reference for an advisory technical opinion.[23]

European Legislation and Regulation of Network Neutrality

European law upholds transparency on a mandatory basis, and minimum Quality of Service on a voluntary basis, under provisions in the 2009 electronic communications framework. Both the 28 Member States, European Economic Area members and the 47 members of the Council of Europe must also conform to the human rights law of the European Convention on Human Rights[24]. This is supplemented in the European Union by data protection legal instruments which are implemented using both the decisions of national and European courts[25], and taking account of the advice of the group of European Union privacy commissioners[26]. In 2011, the European Data Protection Supervisor expressed his concern that traffic management would result in exposure of users' personal data including IP addresses[27]. The CoE also issues various soft law instruments to guide member states in observance of citizens' rights to privacy and free expression[28].

20FCC (2009) *Report on a Rural Broadband Strategy*, 22 May 2009, at pp 15–17 especially footnotes 62–63.

21FCC (2010) *Report and Order Preserving the Open Internet*, 25 FCC Rcd 17905.

22Frieden, Rob (2012) Rationales for and Against Regulatory Involvement in Resolving Internet Interconnection Disputes 14 Yale J.L. & Tech 266 at: http://yjolt.org/sites/default/files/FriedenFinal.pdf

23Broadband Industry Technical Advisory Group (2011) *By-laws of Broadband Industry Technical Advisory Group* Section 7.1

24See Koops, Bert-Jaap and Sluijs, Jasper P. (2012) *Network Neutrality and Privacy According to Art. 8 ECHR*, European Journal of Law and Technology 2(3); at http://dx.doi.org/10.2139/ssrn.1920734; Sluijs, Jasper P. (2012) *From Competition to Freedom of Expression: Introducing Art. 10 ECHR in the European Network Neutrality Debate*, Human Rights Law Review 12(3) at http://dx.doi.org/10.2139/ssrn.1927814

25See Case C-461/10: *Bonnier Audio AB and others v Perfect Communication Sweden* AB, OJ C 317, 20/11/2010 P. 0024—0024 final judgment 19 April 2012 at http://curia.europa.eu/juris/document/document.jsf?doclang=EN&text=&pageIndex=0&mode=DOC&docid=121743&cid=848081.

26Marsden C. [2012] *Regulating Intermediary Liability and Network Neutrality*, Chapter 15, pp701-750 in 'Telecommunications Law and Regulation' (Oxford, 4th edition)

27European Data Protection Supervisor (2011) *Opinion on net neutrality, traffic management and protection of privacy and personal data*

28See *Declaration of the Committee of Ministers on network neutrality adopted 29/9/2010: 1094th meeting of the Ministers' Deputies, a soft law instrument to guide member states in the application of net neutrality rules: aspirations of Articles 6/8/10 of the Convention*

In its initial explanation of its reasons to review the raft of 2002 Directives, the Commission noted the US debate but did no more than discuss the theoretical problem.[29] Over 2007–8, the volume of regulatory reform proposals in the USA, Japan, Canada, and Norway had grown along with consumer outrage at ISP malpractice and misleading advertising, notably over notorious fixed and mobile advertisements which presented theoretical laboratory maximum speeds on a dedicated connection with no-one else using it and subject to 'reasonable terms of usage'—which meant capacity constraints on a monthly basis, some of these on mobile as low as 100MB download totals.[30]

Net neutrality amendments in 2009 Directives

Net neutrality became a significant issue, together, with graduated response, in the voting on the First Reading of the 2009 telecoms package, in May 2009. The European Parliament voted down the reforms at First Reading prior to imminent parliamentary elections in June. Amendments on consumer transparency and network openness were offered to the Parliament in the Conciliation process, collated in the European Commission 'Declaration on Net Neutrality',[31] appended to 2009/140/EC:

> 'The Commission attaches high importance to preserving the open and neutral character of the Internet, taking full account of the will of the co-legislators now to enshrine net neutrality as a policy objective and regulatory principle to be promoted by [NRAs] (Article 8(4)(g) Framework Directive), alongside the strengthening of related transparency requirements (Articles 20(1)(b) and 21(3)(c) and (d) Universal Service Directive) and the creation of safeguard powers for [NRAs] to prevent the degradation of services and the hindering or slowing down of traffic over public networks (Article 22(3) Universal Service Directive).'

There in summary are the concerns about ISPs discriminating against content they dislike, or in favour of affiliated content. The new laws which became effective in Member States in May 2011[32] states that Member States may take action to ensure particular content is not discriminated against directly (by blocking or slowing it), or indirectly (by speeding up services only for content affiliated with the ISP). Note that as network neutrality extends to all consumer ISPs symmetrically, it may not be subject to competition law assessments of dominance, as abuse of dominance is not necessarily an accurate analysis of the network

29COM (2006) 334 *Review of the EU Regulatory Framework for electronic communications networks and services*, Brussels, 29 June 2006 at section 6.2–6.4.

30Leading to a significant emphasis on net neutrality in SEC(2007) 1472 *Commission Staff Working Document: Impact Assessment* at 90–102.

31European Commission, Declaration on Net Neutrality, appended to Dir 2009/140/EC, O J L 337/37 at p 69, 18 December 2009 at <http://eur-lex.europa.eu/LexUriServ/LexUriServdo?uri=OJ:L:2009:337:0037:0069:EN:PDF>

32Directive 2009/136/EC (the 'Citizens Rights Directive') and Directive 2009/140/EC (the 'Better Regulation Directive') both of 25 November 2009, which must be implemented within 18 months.

neutrality problem, at least in Europe.[33] Dominance is neither a necessary nor sufficient condition for abuse of the termination monopoly to take place, especially under conditions of misleading advertising and consumer ignorance of abuses perpetrated by their ISP.[34]

This Declaration, and the more legally relevant Directive clauses, will rely heavily on the implementation at national level and proactive monitoring by the Commission itself, together with national courts, and privacy regulators where content discrimination contains traffic management practices which collate personal subscriber data.[35] Nevertheless, it lays out the principle of openness and net neutrality. The Commission itself adds that it will introduce 'a particular focus on how the 'net freedoms' of European citizens are being safeguarded in its annual Progress Report to the European Parliament and the Council'.[36] Article 22(3) of the Universal Service Directive, stipulates that regulatory authorities should be able to set minimum quality-of-service standards: 'In order to prevent the degradation of service and the hindering or slowing down of traffic over networks, Member States shall ensure that [NRAs] are able to set minimum quality of service requirements'.

Interpretation by BEREC

The European Commission closed its consultation on network neutrality implementation on 30 September 2010[37]. BEREC's response[38] concluded that mobile should be subject to the net neutrality provisions, listing some breaches of neutrality: 'blocking of VoIP in mobile networks occurred in Austria, Croatia, Germany, Italy, the Netherlands, Portugal, Romania and Switzerland'.[39] BEREC explained:

> mobile network access may need the ability to limit the overall capacity consumption per user in certain circumstances (more than fixed network access with high bandwidth resources) and as this does not involve selective treatment of content it does not, in principle, raise network neutrality concerns.'[40]

33 See Marsden (2010) at p 1.

34Some authors question the distinction between degrading and prioritizing altogether, as they find that the latter naturally presupposes the former. See, eg Filomena Chirico, Ilse Van der Haar and Pierre Larouche, 'Network Neutrality in the EU', TILEC Discussion Paper (2007), <http://ssrn.com/abstract=1018326>.

35See Directive 95/46/EC of 24 October 1995, OJ L 281/31 (1995); Directive 2002/58/EC, OJ L 201/37 (2002); Directive 2006/24/EC OJ L105/54 (2006).

36Ibid.

37<http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/net_neutrality/index_en.htm>

38BoR (10) 42 BEREC Response to the European Commission's consultation on the open Internet and net neutrality in Europe, at <http://www.erg.eu.int/doc/berec/bor_10_42.pdf>.

39BoR (10) 42 at p 3.

40BoR (10) 42 at p 11.

They explain that though mobile will always need greater traffic management than fixed ('traffic management for mobile accesses is more challenging'[41]), symmetrical regulation must be maintained to ensure technological neutrality: 'there are not enough arguments to support having a different approach on network neutrality in the fixed and mobile networks. And especially future-oriented approach for network neutrality should not include differentiation between different types of the networks.'

BEREC in December 2011 published its guidelines on transparency and QoS[42]. This is the type of detailed guidance that the subject called out for, including for instance Network Performance (ie what ISPs can actually be monitored for).[43] NRAs have to implement net neutrality in 2013-14 with such detailed guidance. However, on transparency, 'BEREC states that probably no single method will be sufficient'[44] and points out the limited role of NRAs. Governments' consumer and information commission bodies are likely to also play a key role.

BEREC note that legal provisions in the Directives permit greater 'symmetric' regulation on all operators, not simply dominant actors, but ask for clarification on these measures: 'Access Directive, Art 5(1) now explicitly mentions that NRAs are able to impose obligations "on undertakings that control access to end-users to make their services interoperable"'. Furthermore, the new wider scope for solving interoperability disputes may be used in future. This repairs a lacuna in the law, in that the 2002 framework did not permit formal complaints to be made by content providers regarding their treatment by ISPs.

Interpretation by other European institutions

Telecommunications regulators are aware that net neutrality is a more important issue than they are equipped to explore, as the technologies at stake are technologies of censorship.[45] Private Internet censorship, consistent with Article 10(2) ECHR, may only in limited circumstances be acceptable. Note that the introduction of network neutrality rules into European law was under the rubric of consumer information safeguards and privacy regulation, not competition policy.

One of the several principles of network neutrality promulgated by both the FCC and European Commission is that only 'reasonable network management' be permitted, and that the end-user be informed of this reasonableness via clear information. Both the FCC in the US and the European Commission have relied on non-binding declarations to make clear their intention to regulate the 'reasonableness' of traffic management practices. In Canada, the CRTC has relied on inquiries to the dissatisfaction of advocates, while in Norway and Japan

41Ibid.

42Documents BoR 53(11) Quality of Service and BoR 67(11) Transparency, at <http://erg.eu.int/documents/berec_docs/index_en.htm>.

43See BoR 53 [11] at p 3.

44See BoR 67 [11] at p 5.

45BoR (10) 42 at p 20.

non-binding self-regulatory declarations have been thus far non-enforced. Little was done to define reasonableness and transparency by the European Commission prior to the implementation deadline. This has led to extensive and prolonged criticism by the European consumers' organisation, and a substantial package of measurement, consumer empowerment and regulation for greater transparency and consumer rights in the proposed 2013 reforms (discussed below).

National Regulation since 2010: UK, France, Netherlands, Slovenia

Ofcom confined itself to measuring ISP broadband performance, and making it easier for consumers to switch to rival providers. Ofcom has continually attempted since 2008 to reach a self-regulatory solution, creating the unedifying spectacle of appearing to drag unwilling ISPs to the table to agree on what is at least formally 'self-regulation' though with the strongest of regulator pressure applied. Ofcom tried to encourage industry self-regulation via transparency Codes of Conduct, which were unconvincing as recalcitrant industry players agreed to only minimal restrictions on arbitrary limits on consumers' behaviour. By 2011, with implementation of 2009/140/EC needed, the government-funded Broadband Stakeholder Group (BSG) finally produced a Code of Conduct. The UK Ofcom Draft Annual Plan 2012–13 had a small section on traffic management which is bland and uninformative,[46] but promised that Ofcom would 'undertake research on the provision of "best-efforts" internet access.'

France also conducted extensive consultation on net neutrality. Having consulted extensively over an entire year on how to implement the 2009 framework on net neutrality[47], ARCEP in 2010 released a '10 point' principles for net neutrality[48]. ARCEP updated their '10 points' in a report to the French parliament in 2012 which concluded that competition and transparency was insufficient to deal with potential long-term consumer detriments from anti-neutrality behaviours[49]. It concluded that further legislation of the type passed in Netherlands and Slovenia would be required in order to stop blocking and throttling, especially of VOIP over mobile networks, but that this was of course Parliament's competence. ARCEP's position has been that managed services would be permitted to be offered alongside open Internet access, "provided that the managed service does not degrade the quality of Internet access below a certain satisfactory level, and that vendors act in accordance with existing competition laws and sector-specific regulation" (Principle 4 of 2010). It confirmed this stance in permitting an agreement for preferential access to France Telecom/Orange and Free's services by Google's

46Ofcom (2012) Draft Annual Plan 2012/13 at paragraphs 5.40–5.42.

47See further Curien, N. and W. Maxwell (2010) *Net Neutrality in Europe: An Economic and Legal Analysis*, Concurrences, Review of competition laws, N°4.

48ARCEP (2010) *Internet and network neutrality: proposals and recommendations* at www.arcep.fr/uploads/tx.../net-neutralite-orientations-sept2010-eng.pdf

49ARCEP (2012), "Report to Parliament and the Government on Net Neutrality", http://www.arcep.fr/uploads/tx_gspublication/rapport-parlement-net-neutrality-sept2012-ENG.pdf

YouTube content delivery network (CDN) in early 2013[50]. It is important to note that this is a non-neutral provision for a higher speed 'managed service', to which we return in section 8. Furthermore, the competition authority in September 2012 demanded that France Telecom clarify the relationship between its wholesale and retail operations in order to ensure it did not cross-subsidise and margin squeeze competitors, notably Cogent Communications[51]. This has been noted with approval by expert telecoms analysts, with Robinson stating "ARCEP is therefore calling for the elimination of the blocking of VoIP and P2P traffic. The regulator concludes that QoS is a crucial long-term issue that must be monitored in order to "strengthen competitive emulation"[52].

US operators active in the French market did not wish to reveal their traffic data. On 10 July 2013[53], the Conseil d'Etat confirming ARCEP's decision of 29 March 2012 on gathering information on the technical and pricing conditions governing interconnection and data routing, and denied the appeal of US ISPs Verizon and AT&T and their French subsidiaries[54]. ARCEP argued that:

> "regular, twice-yearly information gathering campaigns were vital to the regulator's ability to ensure that these markets run smoothly over time from a technical and economic perspective, particularly in relation to ARCEP's ability to settle any possible disputes that might arise between ISPs and providers of public online communication services."

The decision to uphold the information-gathering demands of ARCEP means that the French regulator will be able to gather more information on the traffic management practices of Tier 1 ISPs and CDNs such as Google than any other national regulator, including those outside the European Union[55]. Arguably it also means that ARCEP will be placed in the best European position to assess the state of competition in the backbone IP interconnect market.

50DSL Prime (2012) *France Telecom, Free To Google YouTube: You're Blocked Unless You Pay*, 27 December at http://www.dslprime.com/dslprime/42-d/4881-france-telecom-free-to-google-youtube-youre-blocked-unless-you-pay

51Autorite de la concurrence (2012) 12-D-18 L. 464-2 at http://www.autoritedelaconcurrence.fr/user/avisdec.php?numero=12D18

52Robinson, James (2012) *ARCEP favors an uncomplicated, flexible approach to net neutrality*, September 28, Ovum Update, at http://ovum.com/2012/09/28/arcep-favors-an-uncomplicated-flexible-approach-to-net-neutrality/

53Conseil d'Etat (2013) Decision No. 360397/360398 of 10 July 2013, at http://arcep.fr/fileadmin/uploads/tx_gsactualite/CE36313071014170.pdf

54ARCEP decision No. 2012-0366 of 29 March 2012

55See ARCEP (2013) at http://arcep.fr/index.php?id=8571&tx_gsactualite_pi1%5Buid%5D=1616&tx_gsactualite_pi1%5Bannee%5D&tx_gsactualite_pi1%5Btheme%5D&tx_gsactualite_pi1%5Bmotscle%5D&tx_gsactualite_pi1%5BbackID%5D=26&cHash=af231efe682036dbe00ed2317f1a9dcc&L=1

Netherlands network neutrality regulation was voted on by its Senate on 6 March 2012,[56] which made it the first European nation to formally introduce mandated network neutrality. The law was delayed until the second half of 2013 by the need for secondary legislation from the Ministry mandating the regulator to implement the law.

Slovenia also passed a law mandating net neutrality, on 28 December 2012, which is on its face more restrictive than the Netherlands law[57]. This was also due for implementation in 2013. Field research is needed to examine the effectiveness of such laws and their operator and consumer effects[58].

2013 Proposed European Regulation

On 11 September 2013, the European Commission adopted a proposed regulation that would substantially impact and harmonise net neutrality provision, allowing priority 'specialized services' and generally preventing ISPs from blocking or throttling third party content[59]. The proposal was extensively strengthened from a July 2013 draft, and its essential items are in part positive and in part negative for net neutrality policy.

Net neutrality 'heavy' is explicitly rejected in a definition of Assured Service Quality[60], in Article 2.12 of the draft law: "assured service quality (ASQ) connectivity product" means a product that is made available at the internet protocol (IP) exchange, which enables customers to set up an IP communication link between a point of interconnection and one or several fixed network termination points, and enables defined levels of end to end network performance for the provision of specific services to end users on the basis of the delivery of a specified guaranteed quality of service, based on specified parameters".

Article 23(5) enforces net neutrality 'lite', thus conforming to the Netherlands and Slovenian laws[61]: "Within the limits of any contractually agreed data volumes or speeds for internet access services, providers of internet access services shall not restrict the freedoms provided for in paragraph 1 by blocking, slowing down, degrading or discriminating against specific

56Netherlands: Senate will debate net neutrality law 6 March 2012 <http://www.eerstekamer.nl/wetsvoorstel/32549_implementatie_van_herziene>

57Article 203(4) of Slovenian Law on Electronic Communications, No. 003-02-10/2012-32, 20 December 2012, http://www.uradni-list.si/1/content?id=111442 Helpful translation of key aspects at https://wlan-si.net/en/blog/2013/06/16/net-neutrality-in-slovenia/

58The author has conducted personal interviews with the relevant national experts in April 2013 (Netherlands) and June 2013 (Slovenia) as well as the Minister responsible in Slovenia (August 2013) and consumer representatives (June 2013). More such research with operators and consumer groups is needed.

59COM(2013) 627 final 2013/0309 (COD) Proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent

60The ASQ definition, also in Annex II of Com(2013) 627 is taken from the ETICS project (2010-12): https://www.ict-etics.eu/overview/objectives.html

61Supra n.57 and Article 7.4a(3) of the Netherlands Telecommunications Act 2012, translated by the Dutch government at http://www.government.nl/files/documents-and-publications/notes/2012/06/07/dutch-telecommunications-act/tel-com-act-en-versie-nieuw.pdf (not official legal translation).

content, applications or services, or specific classes thereof, except in cases where it is necessary to apply reasonable traffic management measures."

Specialized Services: The Exception to Net Neutrality

ISPs are creating managed service lanes alongside the public Internet, with guaranteed Quality of Service (QoS). As the FCC Open Internet Advisory Committee (OIAC) states: "The business case to justify the investment in the expansion of fiber optics and improved DSL and cable technology which led to higher broadband speeds was fundamentally predicated upon the assumption that the operator would offer multiple services"[62]. In its Comast/NBC merger conditions, FCC held that Specialized Service means:

> any service provided over the same last-mile facilities used to deliver Broadband Internet Access Service other than (i) Broadband Internet Access Services [BIAS], (ii) services regulated either as telecommunications services under Title II of the Communications Act or as MVPD services under Title VI of the Communications Act, or (iii) Comcast's existing VoIP telephony service[63].

The FCC Order of 2010 offers a definition of:

> services that share capacity with broadband Internet access service over providers' last-mile facilities, and may develop and offer other such services in the future. These 'specialized services,' such as some broadband providers' existing facilities-based VoIP and Internet Protocol-video offerings, differ from broadband Internet access service and may drive additional private investment in broadband networks and provide end users valued services, supplementing the benefits of the open Internet.[64]

BEREC offers a different definition, more rigorous in enforcing separation from the public Internet:

> electronic communications services that are provided and operated within closed electronic communications networks using the Internet Protocol. These networks rely on strict admission control and they are often optimised for specific applications based on extensive use of traffic management in order to ensure adequate service characteristics.[65]

62Federal Communications Commission Open Internet Advisory Committee (2013) *Annual Report* Released August 20, 2013, at p68.

63Federal Communications Commission (2011) MB Docket No. 10-56, FCC 11-4, pg. 121, at http://www.fcc.gov/document/applications-comcast-corporation-general-electric-company-and-nbc-universal-inc-consent--20

64Supra n.21 at paragraph 112.

65BoR (12) 131 *Guidelines for quality of service in the scope of net neutrality* Document date: 26.11.2012, p5

BEREC explained it: "might be the case that all IAPs present in the access markets are blocking traffic of special P2P applications. That situation might be considered as collective SMP, which is difficult to prove."[66] It went on in paragraph 279 to observe that "Blocking P2P systems or special applications reduces consumers' choice, restricts their efficient access to capacity-intensive and innovative applications and shields the user from innovation. Thus it reduces the consumer's welfare, statically and dynamically." It concludes at paragraph 307 that "For a vertically integrated IAP, a positive differentiation in favour of its own content is very similar to a specialised service." This is an important conclusion, that specialized services can in reality form a means of evading net neutrality regulations, while diverting traffic away from the public Internet to a less regulated premium priced alternative. It created substantial controversy in the US where Comcast was accused of failing to conform to its obligations not to favour its own specialized IPTV service in 2012-13, while under the terms of its 2011 merger consent from the FCC[67]. As with all telecoms licensing conditions, net neutrality depends on the physical capacity available, and it may be that *de facto* exclusivity results in some services for a limited time period as capacity upgrades are developed. Regulations passed in licensing can affect network neutrality at a fundamental level. Interoperability requirements can form a basis for action where an ISP blocks an application.

As the FCC OIAC explains "A high threshold or cap may represent an additional factor that shapes the ability of an edge provider to supply its service or conduct business with a user. If an ISP imposes a data cap or other form of UBP, this could affect user demand for the edge provider's service, which, in turn, may shape the ability of the edge provider to market and deliver its service[68]. This is especially so if the ISP offers specialized services that compete with the edge provider, and for which a cap or other UBP does not apply"[69]. They continue "There is a rationale for separately provisioning between the specialized and non-specialized services, usually to achieve some engineering or market objective, such as improve the quality of service (e.g., reduce user perceptions of delay). In addition, one service often has a set of regulatory requirements associated with it, and one often does not." The conclusion is

> a specialized service should not take away a customer's capacity to access the Internet. Since statistical multiplexing among services is standard practice among network operators, the isolation will not be absolute in most cases. However, if a specialized service substantially degrades the BIAS service, or inhibits the growth in BIAS capacity over time, by drawing capacity away from the capacity used by the BIAS,

66BoR (12) 132 *Differentiation practices and related competition issues in the scope of net neutrality*: Final report, of 26 November, at paragraph 277.

67See Public Knowledge (2013) *Re: Public Knowledge Petition in MB Docket No. 10-56*, p2 at http://www.publicknowledge.org/files/PK%201%20Year%20Letter%20on%20Comcast%20Xbox%20Petition.pdf: "the Commission must show that it has the conviction to actually enforce merger conditions – not merely to impose them".

68See Lee, Timothy B. (2012) May 2, "Sony: Internet video service on hold due to Comcast data cap," Ars Technica http://arstechnica.com/tech-policy/2012/05/sony-warns-comcast-cap-will-hamper-video-competition/

69Supra n.62 at p18.

this would warrant consideration by the FCC to further understand the implications for the consumer and the possible competitive services running on the BIAS service[70].

As FCC OIAC admits in suggesting technology neutrality be observed where possible (2013: 70) "There are painful edge-conditions to this principle, which we acknowledge." There will be substantial controversy regarding definition of specialized services, data caps on public Internet (or 'BIAS' as the FCC calls it), and the limits of public net neutrality rules. This is already apparent in the US, and will be a central feature of the European net neutrality debate in 2014.

Conclusion: Towards a new European Law on Net Neutrality?

The decision to adopt a net neutrality 'lite' approach is that which had been anticipated ever since the 2009 package was voted through the College of Commissioners on 11 September 2013 and is now in negotiation between the institutions. It enables incumbent telcos and others to charge for higher quality but maintains some baseline of free public Internet services. It may require the revision of the Dutch and Slovenian laws, but will take direct effect – should the Regulation actually be enacted – elsewhere far more rapidly than the national regulatory debate otherwise promised. However, the debates in the European Parliament may yet see revision or even blocking of the proposed Regulation between autumn 2013 and spring 2014 (Parliament will be dissolved and a new European Parliament will be elected in May 2014). It is therefore unclear whether this lite-heavy compromise will survive the politics of the winter 2013/14.

There remains an important research question aside from specialized services. One of the main claims by ISPs wishing to traffic manage is that Internet traffic growth is unmanageable by traditional means of expansion of bandwidth and that therefore their practices are reasonable. In order to properly research this claim, regulators and legislators need access to ISP traffic measurement data. There are several possible means of accessing data at Internet Exchange (IX) points, but much data is private either because it is between two peers who do not use an exchange, or because it is carried by a Content Delivery Network (CDN). The delays to the network may make it unreliable for video gaming or voice over the Internet. Regulators are beginning to engage with measurement companies to analyse real consumer traffic[71], and more research into the reality of the consumer broadband experience is much needed. The most recent reliable commercial data suggests Western European fixed Internet traffic is growing at only 17% CAGR and mobile at 50% or lower (the latter number is inherently unreliable as mobile is only 0.15% of overall Internet traffic and networks

70Supra n.62 at p68.

71For instance UK, US regulators and the European Commission employed SamKnows to conduct wide-ranging measurement trial, while Akamai and Cisco issue quarterly 'state of the Internet' traffic aggregation studies. European Commission (2013) *Quality of Broadband Services in the EU: March 2012*, contracted to SamKnows with Contract number: 30-CE-0392545/00-77; SMART 2010/0036. ISBN 978-92-79-30933-5 DOI: 10.2759/24341

jealously guard actual data use)[72]. Both are historically low figures, suggesting the opposite of a 'data explosion'. In order to properly research this claim, regulators and researchers need access to ISP traffic measurement data. There are several possible means of accessing data at Internet Exchange points, but much data is private either because it is between two peers who do not use an exchange, or because it is carried by a CDN[73]. Evidence-based policy-making is sorely needed in this area.

72 Cisco (2012)*Visual Networking Index*, at http://www.cisco.com/en/US/netsol/ns827/networking_solutions_sub_solution.html

73 Faratin, P. et al (2008) *The Growing Complexity of Internet Interconnection*, Communications & Strategies, (72): 51, 4th Quarter at SSRN: http://ssrn.com/abstract=1374285

Privatised Online Enforcement Series

by Joe McNamee

Introduction: Privatised enforcement & net neutrality

The five articles below briefly describe the issue of privatised law enforcement in the digital environment from a variety of perspectives. These problems become more complex and pronounced when the issue of "net neutrality" are discussed. Governments generally want to maintain the open nature of the Internet, because it was this openness that generated such benefits for freedom of communication, for democracy and, indeed, for the economy. This desire has led to countries like the Netherlands seeking to enshrine protection for net neutrality in law. However, governments, faced with the complexity of regulation of online communications, are frequently drawn to the simplistic and cheap "solutions" that demand that industry do "something" to address particular public policy concerns.

It is logically impossible for governments to simultaneously demand that Internet companies – whether online companies providing search facilities or Internet access providers – simultaneously refrain from interfering with information flows (i.e. enforce neutrality), when such interferences are motivated competitive advantage *and* actively engage in interferences if the think, or guess or hope that such interferences will serve the achievement of some public policy goal. It is also either naive or reckless to hope that (often foreign) companies' assessments of what such non law-based interferences with freedom of communication are necessary and proportionate are – and will continue to be - in line with the needs and values of the society. Often, increased government pressure to "do something" skews this balance still further, leaving the Internet company with the task of guessing what action will distract government attention and not take whatever action might be reasonably necessary and proportionate.

A. Abandonment Of The Rule Of Law

This article is looking at the development of processes for cajoling, obliging or coercing online economic operators to police the Internet. At first this article examines the scale of this trend.

Most western democracies either actively or passively recognise that they are based on the "rule of law" and protection of fundamental rights is normally provided within this framework.

In the EU, for example, the rule of law is affirmed four times in the *Treaty on European Union*. It is "confirmed" in the preamble[1] of the Treaty and restated in Article 6[2]. The EU also places an obligation on itself to contribute to the objective of consolidating "democracy and the rule of law" in its development policy (Article 21)[3] and common foreign and security policy (Article 22)[4]. Furthermore, the *European Convention on Fundamental Rights*[5] and the *Charter of Fundamental Rights*[6] place obligations on EU Member States and on the Commission (ratification of the ECHR is pending) that restrictions to freedoms must be based[7] on law[8]. The 2003 Interinstitutional Agreement[9] on better lawmaking which was agreed between the Commission, Parliament and Council further requires in Article 17[10] that self-regulation must respect criteria of representativeness of the parties involved and *"will not be applicable where fundamental rights or important political options are at stake*[11]*"*.

All of these obligations have not prevented the European Commission from[12]:

- Launching a "dialogue" with industry on filesharing, which included proposals from the European Commission on "voluntary" mass filtering of networks by ISPs[13];
- Launching a "dialogue" with industry on "voluntary" deletion of websites accused of containing unlawful material[14] (unless the Internet provider is convinced the site is legal)[15];
- Launching a dialogue on punishments to be meted out by online trading platforms against traders accused of counterfeiting[16];
- Launching a funding proposal for "self-regulatory" blocking of websites accused of containing illegal content[17];

[1] see: Treaty on European Union: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:321E:0001:0331:EN:PDF (1.10.2013)
[2] see: ibid. C 321 E/12 (1.10.2013)
[33] see: ibid. C83/23 (1.10.2013)
[4] see: i.a. ibid.C83/30ff. (1.10.2013)
[5] see: European Convention on Human Rights: http://www.echr.coe.int/Documents/Convention_ENG.pdf (1.10.2013)
[6] see: Charter of Fundamental Rights Of The European Union: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EN:PDF (1.10.2013)
[7] See:European Convention on Human Rights: http://www.hri.org/docs/ECHR50.html, Article 10 (1.10.2013)
[8] see: 2003 Interinstitutional Agreement: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2003:321:0001:0005:EN:PDF, C321/2 (1.10.2013)
[9] see : ibid. C321/1 (1.10.2013)
[10] 2003 Interinstitutional Agreement: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2003:321:0001:0005:EN:PDF, C321/3 (1.10.2013)
[11] see: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2003:321:0001:0005:EN:PDF
[12] In addition, there are other projects elsewhere in the world and globally, such as the US-led "trans-pacific partnership" and the OECD project on the role of ISPs in achieving public policy objectives.
[13] see: http://www.euractiv.com/infosociety/eu-secret-talks-illegal-download-news-501715 (1.10.2013)
[14] see: ibid.
[15] see: http://www.edri.org/edrigram/number8.15/edri-euroispa-notice-takedown-comission (1.10.2013)
[16] see : http://www.mofa.go.jp/policy/economy/i_property/acta_consolidated_text_101006.pdf, page 7 (1.10.2013)

- Agreeing on a text promoting online policing[18] of copyright by Internet providers in the Anti-Counterfeiting Trade Agreement[19];

- Launching a dialogue with the US Federal Bureau of Investigations on "voluntary" deletion of websites and removal of IP address from ISPs abroad;

- Promoting a reduction in privacy in favour of intellectual property rights in the Commission Communication on enforcement of intellectual property rights;

- Agreeing on a global filtering of mobile Internet access with European GSM Operators, in the absence of an identified problem and, in the three years since the agreement was reached, any assessment of its impact;

- Agreeing on a text in the EU/Korea Free Trade Agreement which risks removing core aspects of ISP liability safe harbours, increasing the likelihood of ISPs feeling the need to take pre-emptive punitive measures against consumers suspected of illegal activity;

- Financially supporting an initiative to block funding to websites accused of illegal activity (the model used by Mastercard to block funding to Wikileaks and by Visa to block funding to websites accused of facilitating copyright infringement)[20].

B. Is "Self-Regulation" Worse Than Useless?

Much of the policy with regard to "self-regulation" in the context of illegal online content is developed on the basis that anything that industry can do to help fight crime is automatically a good thing[21]. The assumption is that, however distasteful it is that private companies should be regulating and enforcing the law in the online world[22], it is better that "somebody" is doing "something". The reality is, however, very different.

The first area where Internet intermediaries started enforcing the law is in relation to child abuse images[23]. The European Commission funds "hotlines" to receive reports of child abuse images and these send reports to law enforcement authorities and Internet hosting providers and, sometimes, Internet access providers. Law enforcement authorities are supposed to play their role in investigation and prosecution, while Internet providers are supposed to play their

[17] see: http://www.edri.org/edrigram/number8.15/edri-euroispa-notice-takedown-comission (1.10.2013)
[18] see : http://ec.europa.eu/home-affairs/funding/isec/call_10132/tc2_call_2010_en.pdf, page 3
[19] see: http://www.mofa.go.jp/policy/economy/i_property/acta_consolidated_text_101006.pdf (1.10.2013)
[20] http://europa.eu/rapid/press-release_IP-09-342_en.htm (1.10.2013)
[21] https://www.iwf.org.uk/assets/media/annual-reports/Internet%20Watch%20Foundation%20Annual%20Report%202010%20web.pdf, page 2ff. (1.10.2013)
[22] see: i.a. ibid., page 1ff. (1.10.2013)
[23] http://www.edri.org/files/Written_Statement_Underbjerg.pdf, page 1ff. (1.10.2013)

role, in diligently and within the rule of law, removing content that has been shown to be illegal and supporting collection of evidence by law enforcement authorities[24].

At a recent meeting of the European Commission "dialogue" on dissemination of illegal content within the European Union, the *Safer Internet Unit* of the Commission gave a different and more worrying analysis[25]. A representative explained that many EU police forces did not prioritise online child abuse and even if it was on the priority list in some countries, it was at the bottom. The proposal was made, therefore, that hotlines should send reports directly to Internet hosting providers to delete the websites[26]. The fact that this would facilitate and propagate the alleged inaction of the police appears not to be a consideration.

This approach is confirmed by the European Commission's guidelines for co-funded hotlines on notice and takedown[27] (that are, unsurprisingly, not publicly available), which suggest that agreements should be signed between the hotlines and the police. These guidelines suggest that "the agreement should preferably stipulate a deadline for the police to react after which the hotline would proceed with giving notice". In other words, law enforcement authorities would be assured that, if they remained wholly inactive for an agreed period, the evidence of their failure to address serious crimes would be diligently hidden by the hotlines, in cooperation with well-meaning "industry self-regulation"[28].

This is, unfortunately, far from the only example. As mentioned above, hotlines also contact Internet access providers. In some countries, these take it upon themselves to undertake technically limited "blocking" against sites identified as being illegal[29]. In Sweden, for example, ISPs "block" sites and receive an updated list from the police every two weeks. The pointlessness of this whole process is shown by the fact that, while the lists are updated every 14 days, the British hotline, the IWF, has produced statistics showing that the average length of time the sites remain online is only twelve days[30]. In other words, on average, there are no functioning sites at all on the "blocking" list[31] one day out of every seven.

Unfortunately, this activity is not just useless, it is worse than useless. In a speech given to the German Parliament, a Danish police official explained that, having "blocked" the websites domestically, the police in that country do not see any point in communicating evidence of serious crimes against children to the police forces in the United States and

[24] https://www.iwf.org.uk/assets/media/annual-reports/Internet%20Watch%20Foundation%20Annual%20Report%202010%20web.pdf, page i.a. 3ff. (1.10.2013)
[25] http://www.circamp.eu/index.php?option=com_content&view=article&id=24:interpol-crimes-against-children-team-on-eu-directive (1.10.2013)
[26] https://www.iwf.org.uk/assets/media/annual-reports/Internet%20Watch%20Foundation%20Annual%20Report%202010%20web.pdf page 2ff. (1.10.2013)
[27] http://www.edri.org/edrigram/number8.15/edri-euroispa-notice-takedown-comission (1.10.2013)
[28] https://www.iwf.org.uk/assets/media/annual-reports/Internet%20Watch%20Foundation%20Annual%20Report%202010%20web.pdf page 2ff. (1.10.2013)
[29] see : ibid. (1.10.2013)
[3030] http://www.edri.org/files/Written_Statement_Underbjerg.pdf (1.10.2013)
[31] http://www.circamp.eu/index.php?option=com_content&view=article&id=24:interpol-crimes-against-children-team-on-eu-directive (1.10.2013)

Russia, because they probably wouldn't be interested. It is difficult to imagine another crime which would be treated in such a trivial way.

Reports from the European Commission are that there will be a major push to increase the *"safer internet"* budget, which is currently being reviewed. As yet, there are no signs that any lessons are being learned regarding the failures of "self-regulation" under the current programme.

C. The Law According To The Advocate General

The Advocate General of the European Court of Justice recently published his views with regard to the *Scarlet/Sabam* case C-70/10 in the European Court of Justice[32]. This is a crucial case with regard to privatised enforcement, as it is the first time that the legality of this approach has been tested. The case came as a result of an attempt by the Belgian collecting society Sabam to require the small Belgian ISP Scarlet to install a filtering system to monitor all peer to peer traffic on its network and block files which Sabam ruled to be unauthorised[33]. As Scarlet was a small, struggling ISP, Sabam hoped that they would comply to avoid high court costs.

Since the start of the case, however, things have unravelled somewhat for Sabam. Firstly, Scarlet was taken over by the Belgian former incumbent Belgacom, which had the resources and ability to fight the case and, secondly, Sabam was humiliated by an undercover TV "sting" which showed them demanding royalties for artists that do not exist (such as Suzi Wan, a brand of noodles) and demanding royalty payments for use of their non-existent works.

The Advocate General described the case as being about (paragraph 54) "delegating the legal and economic responsibility of the fight against illegal downloading to Internet access providers." Sabam's action in bringing the case has been very valuable to digital rights. If they had not brought this case, the European Commission would have been vigorously pushing in favour of exactly such measures, claiming that this approach was legal without immediate fear of contradiction.

For example, in the recent Communication on the implementation of the IPR Enforcement Directive[34], the Commission argued that such injunctions might be applied, without contradicting any relevant EU law or human rights law. This is also the advice that it gave to the Court. Indeed, the Commission had already run a "dialogue on illegal up- and downloading" with the industry and the content industry with the aim of achieving "voluntary" breaches of the right to privacy and the right to communication that are at stake in the Scarlet/Sabam case, albeit without success.

[32] http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-04/cp110037en.pdf (1.10.2013)
[33] see: http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-04/cp110037en.pdf (1.10.2013)
[34] see: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0779:FIN:EN:PDF

The view of the Advocate General is that the filtering and blocking demanded by Sabam would constitute an infringement of the fundamental rights to privacy and communication. As such, the requirements imposed by the Charter on Fundamental Rights and Convention of Human Rights in such cases would have to be met. In particular, the Advocate General explains that restrictions must be based on law, the law must pre-date the restriction and the law must be necessary, proportionate and effective[35]. Interestingly (paragraph 113), he also says that Article 52.1 of the Charter creates an implicit obligation for the law to be properly legitimated by a legislative process[36].

In paragraph 52 of the Opinion, the Advocate General explains that, according to the Charter on Fundamental Rights, the proportionality of a restriction of fundamental rights needs to be defined both by the legislator, when formulating the law on which the restriction is based and by the judge imposing the restriction[37]. Not only does this contradict the Commission's input on in this particular case, it also places huge doubts over a wide range of Commission initiatives. For example, in recital 13 of the Child Exploitation Directive, the Commission bizarrely suggests "stimulating" internet providers to undertake blocking and filtering "voluntarily," circumventing the law, the legislator and the judge.

It remains to be seen what lessons the European Commission will take from this ruling in its demands for more extra-judicial policing from Internet intermediaries. In particular, will the Commission stop funding projects, such as CIRCAMP, its entire raison d'etre being in fundamental contradiction with this Opinion?

D. Anatomy Of A Self-Regulation Proposal

How does it happen that an industry or a sector of industry signs up "voluntarily" to arbitrarily punish their consumers and to restrict freedom of speech? One of the most interesting and telling examples is the ongoing "public/private dialogue to fight online illegal activities"[38].

In November 2009, the European Commission Directorate General for Justice Liberty and Security (the relevant units are now part of DG Home Affairs) invited a variety of Internet companies (but no civil society representatives) to a meeting to discuss, in very vague terms, the issue of illegal content online - concentrating on child abuse, terrorism and racism/xenophobia. In that meeting, no particular problem was identified that needed to be solved and various existing approaches were presented to fight such content[39].

[35] http://www.circamp.eu/index.php?option=com_content&view=article&id=24:interpol-crimes-against-children-team-on-eu-directive (1.10.2013)
[36] http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-70/10 (1.10.2013)
[37] See: ibid.(1.10.2013)
[38] see: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailPDF&groupID=622 (1.10.2013)
[39] see: http://www.edri.org/files/Draft_Recommendations.pdf (1.10.2013)

At that meeting, the European Commission offered to prepare draft recommendations to form the basis of future discussions. This text would formally be the Commission's "understanding" of industry's views and not, legally speaking, a proposal from the Commission. As a result, the Commission's proposals would not need to go through either any internal approval systems in the Commission or, being a non-legislative proposal, through the Council of the EU or European Parliament. This loophole permits the Commission to make proposals to industry informally, but with the threat of legislation permanently in the background[40].

The Commission subsequently produced the set of recommendations[41], which listed a variety of circumstances where "Internet providers" could "remove or disable access" to content, without any judicial oversight and without any clear obligations for public authorities to act against the criminally illegal content - a public/private dialogue where the public has to do nothing and the private does everything, outside the democratic process and the rule of law[42].

The Commission then organised another meeting in May 2010, at which EDRi asked to participate. During that meeting, EDRi repeatedly asked for information on what specific problems with illegal content hosted in Europe had been identified that this project sought to address. No response was forthcoming. Industry participants echoed this call and asked why, if the Commission is only talking about hosting providers, it did not make reference to hosting providers rather than "internet providers" in its proposed text. No answer was forthcoming. At the end of that event, the Commission promised to take the concerns into account and to produce a revised set of recommendations. Meanwhile, EDRi and the European ISP Association (EuroISPA) prepared a joint letter explaining the minimum requirements to be respected[43].

In December 2010, another draft recommendation set was put forward by the Commission, which was virtually identical to the one in May. A day-long meeting was organised where the same questions were asked by EDRi and by industry, with the Commission again failing to provide any information regarding the nature of the problem that the process was supposed to solve. After the meeting, EDRi joined with both EuroISPA and the European Telecoms Networks Operators Association (ETNO) to again put the concerns and demands of both civil society and industry in writing. Six months later, the only response that the letter has received is that it would not be answered before June[44].

This whole process has been a solution in search of a problem, exploiting a loophole where individual services in the Commission can make proposals of major importance to freedom of communication without any bureaucratic or democratic oversight using the pretence that they are not Commission proposals at all.

[40] see: http://www.edri.org/files/090710_dialogue_NTD_illegal_content_EuroISPA-EDRI.pdf (1.10.2013)
[41] see: http://www.edri.org/files/Draft_Recommendations.pdf (1.10.2013)
[42] see: http://www.edri.org/files/Draft_Recommendations.pdf (1.10.2013)
[43] see: http://www.edri.org/files/090710_dialogue_NTD_illegal_content_EuroISPA-EDRI.pdf (1.10.2013)
[44] see: ibid. (1.10.2013)

E. Online Trading Platforms Sell Out

In a bizarrely designed document, looking like a mix between a wedding invitation and an accident in a blue ink factory, leading online retailers *Amazon*, *eBay* and *Priceminister* have sold out the interests of their consumers in a "memorandum of understanding" with a range of luxury goods and copyright groups. In return, they have received a non-binding commitment not to be sued by the rightsholders for twelve months[45].
Under the agreement, the Internet platforms agree to take responsibility "to assess the completeness and validity of" reports from rightsholders of counterfeit goods being sold through their services and, based on this extra-judicial notice, not only to remove the listings of the alleged counterfeit material but also to take "deterrent measures against such sellers"[46].

Furthermore, for reasons that are not explicitly explained, Internet platforms will receive lists of words "commonly used for the purpose of offering for sale of 'obvious' counterfeit goods[47]" which they will "take into consideration[48]". Up to the limits imposed by data protection law, "Internet Platforms commit to disclose, upon request, relevant information including the identity and contact details of alleged infringers and their user names[49]".

On the other side, the rightsholders undertake to make requests for personal information "in good faith[50]" and in accordance with the law.
With regard to sellers who are adjudged by the online retailer to have repeatedly broken the law, the Internet platforms undertake to "implement and enforce deterrent repeat infringer policies, according to their internal guidelines[51]" including temporary or permanent suspension of the seller. These deterrent measures are to be implemented taking into account a number of factors, including the "apparent intent of the alleged infringer". The policing by the Internet platforms will, in turn, be policed by the rightsholders who, subject to data protection law "commit to provide information to Internet Platforms concerning those sellers they believe to be repeat infringers and commit to provide feedback to Internet Platforms on the effectiveness of Internet Platforms' policies regarding repeat infringers (e.g. if rights owners feel that there has been a failure to take measures against a repeat infringer).

In the entire document, which consists of 47 paragraphs, just one is devoted to the enforcement of the law by law enforcement authorities[52].

[45] http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf (1.10.2013)
[46] see: ibid. (1.10.2013)
[47] see: ibid. (1.10.2013)
[48] see: ibid. (1.10.2013)
[49] see: ibid.(1.10.2013)
[50] see: ibid. (1.10.2013)
[51] see: ibid. (1.10.2013)
[52] see: http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf. (1.10.2013)

References

A.
2003 Interinstitutional Agreement:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2003:321:00...

Treaty on European Union:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:321E:0...

European Convention on Human Rights:
http://www.hri.org/docs/ECHR50.html

Charter of Fundamental Rights:
http://www.hri.org/docs/ECHR50.html

Dialogue on dissemination of illegal online content:
http://www.edri.org/edrigram/number8.15/edri-euroispa-notice-takedown-...

Filesharing project:
http://www.euractiv.com/en/infosociety/eu-secret-talks-illegal-downloa...

ACTA consolidated text:
http://www.mofa.go.jp/policy/economy/i_property/acta_consolidated_text...

Commission funding proposal:
http://ec.europa.eu/home-affairs/funding/isec/call_10132/tc2_call_2010...

IPR Enforcement Directive Communication:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC077...

Mobile blocking of allegedly illegal content:
http://ec.europa.eu/information_society/activities/sip/events/forum/fo...

OECD project on ISPs and public policy objectives:
http://www.oecd.org/dataoecd/8/59/45997042.pdf

Charter of fundamental rights:
http://www.europarl.europa.eu/charter/pdf/text_en.pdf

EDRi study on "self-regulation":
http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf

Trans-pacific partnership:
http://arstechnica.com/tech-policy/news/2011/03/son-of-acta-meet-the-n...

Blocking of payments:
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/342

EU/Korea Free Trade Agreement:
http://trade.ec.europa.eu/doclib/press/index.cfm?id=443

B.

Internet Watch Foundation Annual Report 2010
http://www.iwf.org.uk/assets/media/annual-reports/Internet%20Watch%20F...

EDRi-gram: Dialogue on illegal online content (28.06.2010)
http://www.edri.org/edrigram/number8.15/edri-euroispa-notice-takedown-...

Child abuse is difficult to stop on the web (only in Swedish, 29.09.2010)
http://www.dn.se/nyheter/sverige/overgrepp-pa-barn-svart-stoppa-pa-nat...

Danish police statement
http://www.edri.org/files/Written_Statement_Underbjerg.pdf

Privatised Online Enforcement Series A. Abandonment of the rule of law
(23.03.2011)http://www.edri.org/edrigram/number9.6/abandonment-rule-of-law

C.

Advocate General's Opinion (14.04.2011)
http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=reche...

Court of Justice Press Release (14.04.2011)
http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-04/cp1100...

Circamp
http://www.circamp.eu

The Suzi Wan playlist
http://www.humo.be/tws/actua/21679-3/basta-vs-sabam.html

EU in "secret talks" to stop illegal downloads (28.01.2011)
http://www.euractiv.com/en/infosociety/eu-secret-talks-illegal-downloa...

D.

EDRi/EuroISPA letter (07.09.2010)
http://www.edri.org/files/090710_dialogue_NTD_illegal_content_EuroISPA...

Commission recommendations (last 4 pages are relevant)
http://www.edri.org/files/Draft_Recommendations.pdf

E.

Memorandum of Understanding (4.05.2011)
http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_040...

A Discourse-Principle Approach to Network Neutrality: A Model Framework and its Application

by Luca Belli and Matthijs van Bergen

The protection of network neutrality ("NN") is a crucial challenge for current information societies. The enshrinement of this all-important principle into policy and legislation appears necessary to foster an open Internet where users are active participants and not mere consumers. Indeed, NN empowers Internet users allowing them not only to freely receive and impart information but also to freely receive and impart innovation. By contrast, in a non-neutral Internet, the power to decide which kind of innovation and information should be accessed and distributed by end-users, would primarily lie with Internet service providers. Such centralised control over Internet traffic flows has the potential to determine nefarious consequences on media pluralism as well as on the circulation of innovation. Therefore, the extent to which the NN principle is safeguarded and implemented has a direct impact on the full enjoyment on human rights online and, therefore, also on the level of accomplishment of democracy and self-determination in the various information societies.

One of the main purposes of the Dynamic Coalition on Network Neutrality (DC NN) was to elaborate a model legal framework on network neutrality that would enable innovation and be consistent with international human-rights standards, while also being 'scalable', which in this context means being easily implemented and applied across different legal systems. To come to such a "Model Framework", the DC NN has adopted a process, grounded on openness, inclusion, transparency and participation. This article will first briefly describe the Habermassian process that the DC NN has tried to put in place and will subsequently highlight the result of such process and its concrete application, whose only aim is to protect NN in an efficient fashion. Subsequently the Model Framework will be presented and its application elaborated.

A Discourse-Principle Approach

According to Jurgen Habermas' discourse principle, the only norms that one can claim to be valid are those meeting – or having the possibility to meet – the approval of all the participants in a practical discourse. Hence, Habermas argues that norms' legitimacy should not be based on their "formal-semantic properties" but should be rather guaranteed by the formal conditions that allow "rational will formation" through participation to this discourse[1].

However, the philosopher acknowledges that, in spite of how sophisticated can be the efforts to achieve a consensual rule on a purely rational basis, human beings' lack of "perfect knowledge" inexorably leaves them in a state of uncertainty regarding whether the rule they

elaborate has truly been crafted according to the discourse principle. For this reason the most suitable solution – or the one with the least hindrance, depending on the point of view – is to undertake a participatory process through which the elaboration of the rule is legitimised by participants' free contribution on an equal basis, in order to put in place "a cooperative search for truth, where nothing coerces anyone except the force of the [most persuasive] argument"[1].

To this latter extent Michael Froomkin has stressed that the achievement of the Habermasian practical discourse depends on how closely the participants to this collaborative effort manage to approach "an ideal in which (1) all voices in any way relevant get a hearing, (2) the best arguments available to us given our present state of knowledge are brought to bear, and (3) only the unforced force of the better argument determines the 'yes' and 'no' responses of the participants"[1]. However, it is important to note that only in an ideal – and particularly difficult to realise – situation it is possible to completely fulfil the aforementioned conditions. Therefore, considering the practical difficulties to realise an ideal practical discourse, "something less than the "best" might be also be a practical discourse"[1].

The Internet-standards elaboration process developed by Internet standardisation bodies, such as the Internet Engineering Task Force (IETF), can be argued to form such a near-fulfilment of the practical-discourse conditions. This process is open to every Internet user and based on the collaborative development of Requests for Comments through a transparent e-mail interaction. The purpose of this continuous email exchange is to facilitate the participatory process that leads to the crystallisation of "rough consensus" through the confrontation of rational arguments. In this way, the proposed standards are commented and refined in order to become draft-standards, ready to be adopted uniquely by reason of their rational efficiency[1].

A Net Neutrality Policy-Blueprint

It should be acknowledged that the participatory process put in place though open, inclusive and transparent email interaction has the potential to make the Habermasian practical discourse a (close) reality. Indeed, although mailing-list debates have obvious benefits and disadvantages[1], it cannot be denied that they can be utilised as a true debate-arenas, aimed at facilitating a "rational-will formation" process, which may be a close approximation of the Habermasian practical discourse.

Such a process is particularly beneficial to highlight the potential implications of Internet-related policy-recommendations through an open dialogue, thus allowing the elaboration of "scalable and innovation-enabling"[1] policies. The Dynamic Coalition on Network Neutrality (DC NN) has therefore been established[1] in order to transpose the practical-discourse approach that characterises Internet standardisation to network neutrality policy-making. Indeed, the structure of the DC NN has intended to reproduce the self-organised, bottom-up and collaborative environment characterising Internet-standardisation bodies. Particularly, the creation of an open, inclusive and transparent discussion-platform has been considered as a fundamental precondition in order to foster the confrontation of rational arguments that is needed to elaborate efficient solutions to safeguard network neutrality. Indeed, both the

technical complexity of the NN debate and the large spectrum of stakeholders, which are involved in the direct and indirect provision of Internet communications, impose to analyse this all-important issue through a participatory and multi-stakeholder process.

The DC NN has tried to establish such a process and the Model Framework on Network Neutrality has been elaborated through exclusive e-mail interaction over a two-month period. The Dynamic Coalition mailing-list has been advertised on several websites and opened to any interested stakeholder. Mailing-list's participants[1] are formally equal, although they can be categorised in 5 stakeholders groups: governmental entities; private-sector entities; non-governmental organisations; technical community; and academia. Mailing-list's discussions have been moderated by a coordinator and one "on-line vote" has been called for in order to solve a terminology controversy[1]. Lastly, the mailing-list archives are freely accessible to every Internet-user.

The first "draft model" has been elaborated utilising elements from two model laws, submitted by Luca Belli and Matthijs van Bergen to the Multi-Stakeholder Dialogue on Network Neutrality and Human Rights, a conference organised under the auspices of the Council of Europe, on 29-30 May 2013. Subsequently, two comment periods – the first one lasting 30 days and the second one 10 – have been foreseen in order to reply to a "Request for Comments" on the draft model and a third, informal comment-period has been established to allow final remarks and objections.

The Model Framework on Network Neutrality is therefore the collaborative product of this cooperative interaction and should be considered as a "policy blueprint" providing guidance to national legislators on how to properly safeguard network neutrality. The adoption of this model framework should be undertaken on a merely voluntary basis and exclusively driven by the efficiency of this instrument.

The Model Framework on Network Neutrality and its Application

The main goal of the Model Framework is to help clarifying the NN debate and to present a way forward. To this end, the first article of the Model aims at bridging a dialectic lacuna, by precisely defining the network neutrality principle. Consequently, the Model delineates the limits of such a crucial principle as well as the criteria according to which it should be applied. Furthermore, the Model suggests an enforcement mechanism which seems essential in order to implement network neutrality in an appropriate fashion.

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 partner;*
- *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, 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.*

The Application of the Model Framework

Article 1 of the Model first defines NN and subsequently explains the aim of this principle. NN is essentially a non-discrimination principle which applies to the transmission of Internet traffic.

According to this principle, all Internet traffic is to be transmitted equally and without discrimination, restriction or interference, regardless of the type or content of the traffic and regardless of the identity of its sender or recipient. Therefore, it may be argued that NN plays a pivotal role in enhancing freedom of choice, freedom of expression, privacy and self-determination of all Internet users, while fostering media pluralism and economic innovation.[1]

In accordance with the network neutrality principle, ISPs must manage Internet traffic in a non-discriminatory fashion. A prime example of a non-discriminatory transmission mode is first-in, first-out, or "FIFO" transmission of Internet packets. Besides FIFO there is a multitude of other queuing and transmission policies that do not depend on the characteristics of specific applications, content, services, devices and uses. Net neutrality prescribes that ISPs must in principle apply only such "application-agnostic"[1] forms of Internet traffic management ("ITM"), while any application-specific discrimination, restriction or interference is only allowed if strictly necessary for and proportionate to any of the legitimate aims listed in article 2. The application of article 2 should be put in place through the following 'five-step test':

1) It should first be established whether or not an interference, restriction or discrimination has occurred. Any ITM that is not application-agnostic should be deemed as a discrimination, restriction or interference (in short: interference);

2) the second step is to determine whether the interference in question is prescribed by the agreement between the ISP and its subscriber. If the agreement does not provide a sufficiently foreseeable ground for the interference, it is illegal. If the interference is prescribed by the agreement, we proceed to step three;

3) the third step consists in establishing whether the interference was applied for a legitimate aim. 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*.

4) 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.

5) 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 measure in order to achieve the same purpose.

Similar to the way the European Court of Human Rights ("ECtHR") leaves a wider or smaller margin of appreciation to member states in certain situations, national 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 about its efficiency or proportionality, the margin of appreciation can be left wider as well.[1]

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.

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. As an example, the blocking of (D)DOS traffic and malware can be mentioned.

Furthermore, it is important to note that in many European jurisdictions –at least in those within the EU – it is forbidden to send unsolicited electronic communications for direct marketing purposes, commonly referred to as "spam".[1] Although the problem of spam can also be dealt with at the 'edge', e.g. by filtering at the mail server, it may be considered wasteful if all spam traffic, which is said to constitute about 70-80 % of all e-mail traffic[1], 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 indent c requires that the least restrictive and least discriminatory method that is still sufficiently effective, is used.

If a subscriber wishes that certain application-specific ITM measures be taken by the ISP, the ISP may comply with such request, in accordance with indent d. 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.

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.

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).

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. However, such business models are not banned *in toto*, for they may be implemented through specialised services. Indeed, in accordance with 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. 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.

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.

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 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'[1].

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.

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.

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[1] 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.

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.

References

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

DeNardis L., *Protocol Politics: The Globalization of Internet Governance*, 2009.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Donley C. *et al., Request for Comments: 7021, Assessing the Impact of Carrier-Grade NAT on Network Applications*, September 2013, available at http://www.rfc-editor.org/rfc/rfc7021.txt

Dynamic Coalition on Network Neutrality, available at: http://networkneutrality.info/ and at: http://www.intgovforum.org/cms/dynamic-coalitions/1330-dc-on-network-neutrality.

Froomkin M.A., "Habermas@discourse.net: Toward a Critical Theory of Cyberspace", in *Harvard Law Review*, Vol 116, n° 3, January 2003.

Habermas J., "Discourse Ethics: Notes on a Program of Philosophical Justification", in Habermas J., *Moral Consciousness and Communicative Action*, 2001.

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

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.

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

Schewick B., *Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like*, June 11, 2012.

Shelly, R., "Habermas and the Normative Foundations of a Radical Politics", in *Thesis Eleven*, no. 35, 1993.

McAuley C., *3 Things You Need to Know About Carrier-Grade NAT*, 14 February, 2012, available athttp://blogs.ixiacom.com/ixia-blog/carrier-grade-nat-testing/

Conclusion

by Luca Belli, Primavera de Filippi and Matthijs van Bergen

The Internet is a complex network of networks, where a number of intermediaries contribute to routing, transferring, and forwarding data-packets often without any obligation or responsibility as regards the speed, performance, or quality of service.

NN is a principle requiring that data-packets be routed and transmitted in a non-discriminatory fashion, regardless of their type, content, origin or destination so that all Internet communications be treated equally, save in narrowly circumscribed exceptional cases. NN can be argued to be enshrined in the original philosophy of the Internet community, grounded on the openness principle and transposed in a robust and decentralised network that allows the pursuit of universal accessibility and connectivity. The Internet-pioneers' philosophy is reflected in the design of the Internet, based on end-to-end principle, whereby the intelligence of the network should primarily be located at its edges. Such design is not only technically robust and 'scalable'; it also empowers end-users, rather than the infrastructure operators. Indeed, the network neutrality principle is fundamental in order to ascribe a proactive role to end-users who, thanks to this all-important principle, are not mere consumers, but rather active participants of a global community.

The technical evolution has delivered a variety of (more or less intrusive) traffic management measures, aimed at improving network operators' capability to define the quality of the service they provide to their user base. Furthermore, the use of certain traffic management techniques is sometimes even required by national legislation in order fulfil some narrowly circumscribed legitimate aims, by blocking access to illegal content.

However, the Report of the Dynamic Coalition on Network neutrality highlights that application-specific traffic management, allowing blocking and/or filtering Internet-traffic relating to specific content, applications, services or devices, holds promise to jeopardise the open architecture of the Internet and to significantly impinge upon user's fundamental rights, such as the right to privacy and freedom of expression. Hence, the implementation of application-specific techniques should be allowed only if they pursue legitimate aims precisely defined by a strict legal framework, and if they are sufficiently efficient and proportionate. Furthermore, the rule-of-law principle demands an accurate framework regulating the scope of any prohibition to access online resources and guaranteeing the respect of the due-process principle in order to prevent possible abuses.

The challenge in the NN debate is to establish the extent to which Internet Service Providers should be entitled to control or manage Internet traffic, without undermining the full enjoyment of end-users' human rights or infringing upon the underlying principles necessary for the preservation of an open and neutral Internet.

The Dynamic Coalition on Network Neutrality has attempted to tackle this challenge and elaborated a "policy blueprint" that aims at providing guidance to legislators on how to safeguard NN in an efficient fashion. The Dynamic Coalition has tried to reproduce the open, inclusive and transparent process that characterises the elaboration of Internet standards and protocols into a policy-making process. Indeed, such a multi-stakeholder and participatory approach seems essential to craft 'scalable' policies that encourage innovation while protecting human rights.

As any standards, the model framework offers a potential solution which is by no means the only one. For this reason, the adoption of the model framework proposed by the Dynamic Coalition should be undertaken on a merely voluntary basis and exclusively driven by the efficiency of this instrument.

Authors

Luca Belli is the founder and co-coordinator of the Dynamic Coalition on Network Neutrality and is currently serving as a Council of Europe Expert on Network Neutrality. 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 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.

Giusy Cannella is Junior Policy Analyst at Access and she is based in Brussels. Giusy is from Italy, but has been living in Brussels for the past three years where she developed experience and insight into the European institutions, notably through her work as a trainee for the First-Vice President of the European Parliament. She also wrote her Master thesis on the EU-US PNR Agreement and on the EU Data Protection Reform Package. Following graduation with honours in EU Politics and Institution, she joined Access to support Brussels' Senior Policy Analyst, focusing on network neutrality.

Primavera De Filippi is a researcher at the CERSA / CNRS / Université Paris II; representative of CreativeCommons France and coordinator of the Public Domain working group at the Open Knowledge Foundation. She is currently a fellow at the Berkman Center for Internet & Society at Harvard University, where she investigate the concept of "governance by design" as it relates to cloud computing and peer-to-peer technologies

Maria Löblich (PhD, communication sciences) is an assistant professor at the Department of Communication Science and Media Research, Ludwig-Maximilians-Universität München. She was part of the fellowship class at the Berkman Center for Internet & Society at Harvard University in the 2012-2013 academic year. Her research focuses on internet policy with a particular interest in political processes and actor-structure interactions.

Raegan MacDonald is Senior Policy Analyst at Access. Originally from Canada, Raegan is based in Brussels, Belgium, and has been representing Access on European policy for the past 2 years. Raegan specialises in privacy and data protection and in network neutrality. She is also an Observer of European Digital Rights (EDRi), an association of 32 privacy and civil rights groups across Europe. Raegan a graduate of the University of Vienna (Austria) and the University of Leipzig (Germany) where she received her Masters in Global Studies; her thesis examined the importance of user privacy in the age of ubiquitous computing.

Christopher T. Marsden is Professor of Media Law at the University of Sussex, since April 2013. He is author of four monographs on Internet law: "Regulating Code" (2013, MIT Press with Dr Ian Brown), "Net neutrality: Towards a Co-Regulatory Solution" (2010, Bloomsbury), "Internet Co-regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace" (2011, Cambridge), "Codifying Cyberspace" (Routledge/Cavendish 2007 with Dr. D. Tambini, D. Leonardi). He was formerly Senior

Lecturer (2008-12) then Professor of Law (2012-13) at Essex, having previously taught and researched at Warwick (1997-2000), Oxford (2004-5), LSE (1995-1997).

Andrew McDiarmid is a Senior Policy Analyst at CDT's Washington, DC, office. He works on policy issues related to digital copyright, free expression, and Internet neutrality. Prior to joining CDT, Andrew was a research assistant at the Samuelson Law, Technology, and Public Policy Clinic at the UC-Berkeley School of Law, where he researched a range of issues including electronic surveillance and licensing solutions for peer-to-peer networks. He has a master's from Berkeley's School of Information, and a bachelor's in art history from Washington University in St. Louis.

Joe McNamee is Director of European Digital Rights, an association of digital civil rights associations from 20 European countries. He holds Master's Degrees in International Law and in European Politics. Prior to joining EDRi, he worked for a consultancy, primarily on Internet regulation issues. He also was responsible for three studies for the European Commission - on local loop unbundling, convergence of telecoms and internet networks and communications markets and regulation in eight former Soviet states. He has a strong interest in industry self-regulation issues, particularly with regard to privatised law enforcement.

Francesca Musiani (PhD, socio-economics of innovation) is currently a post-doctoral researcher at the Centre for the Sociology of Innovation, MINES ParisTech/CNRS. Recently, she was the 2012-13 Yahoo! Fellow in Residence at Georgetown University and an affiliate of the Berkman Center for Internet & Society at Harvard University. She is the author of Nains sans géants. Architecture décentralisée et services Internet (2013, Presses des Mines). Her research explores Internet governance in an interdisciplinary perspective.

Alejandro Pisanty is a professor at the National Autonomous University of Mexico where he has also served as Academic CIO and Coordinator for Open and Distance Education. His education includes a Ph.D. in Theoretical Chemistry and a postdoctoral period in the Max Planck Institute for Solid State Research. He has been a member and Vice-Chair of the ICANN Board of Directors and a Trustee of the Internet Society (ISOC), as well as a member of the Working Group on Internet Governance. He is Chair of ISOC Mexico and a well-known, active scholar, speaker, and promoter in the field of Internet governance. He is also an active blogger and microblogger and has led successful social-media based campaigns like #InternetNecesario

Louis Pouzin is a consultant, giving seminars on internet evolution, is an active participant in the UN Internet Governance Forum, and contributes to several non profit organizations, EUROLINC (native languages in internet), MAAYA (federation for cultural and linguistic diversity), ATENA (high level seminars). He has created a company, Savoir-Faire, for selling new Top Level Domains (Open-Root).

Marietje Schaake is a Member of the European Parliament for the Dutch Democratic Party (D66) with the Alliance of Liberals and Democrats for Europe (ALDE) political group. She serves on the Committee on Foreign Affairs, where she focuses on neighbourhood policy, Turkey in particular; human rights, with a specific focus on freedom of expression, internet

freedom, press freedom; and Iran. In the Committee on Culture, Media, Education, Youth and Sports she works on Europe's Digital Agenda and the role of culture and new media in the EU's external actions. In the Committee on International Trade she focuses on intellectual property rights, the free flow of information and the relation between trade and foreign affairs.

Matthew Shears leads the Center for Democracy and Technology's Global Internet Policy and Human Rights (GIPHR) activities. A UK national, Matthew has extensive experience in Internet and telecommunications policy and governance in the non-profit, public and private sectors. Most recently he assisted CDT's Internet governance and policy work at the World Conference on International Telecommunications (WCIT), the UNESCO World Summit on the Information Society (WSIS) review and the World Telecommunication/ICT Policy Forum (WTPF). From 2005 through 2009, Matthew was the Internet Society's Public Policy Director, responsible for building the global policy team and representing the organization during the Tunis phase of the WSIS, at ITU Telecom World and at the Internet Governance Forum. From 2006-2008 he was a member of the UN Secretary General's Advisory Group on Internet governance.

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 serving as a network neutrality expert for the Council of Europe.

Acknowledgements

This report is the result of a collective work. The Dynamic Coalition on Network Neutrality (DC) has indeed been created to stimulate the debate on network neutrality and this work reflects a small but significant percentage of the ideas that have been exchanged by the DC's members and of the contributions that have been provided by the DC's mailing-list members.

The editors would like to express immense gratitude the Microsoft Corporation (and particularly to Jean-Jacques Sahel for his patience and support), which has made possible to print this book thanks to a generous donation.

Furthermore, the editors would like to thank the *Centre d'Etudes et de Recherches de Sciences Administratives et Politiques* (CERSA), which has always provided support and guidance, stimulating their research efforts.

The editors would also like to thank the Council of Europe for the organisation of the Multi-Stakeholder Dialogue on Network Neutrality, an event that has played a pivotal role in advancing the discussion on network neutrality and has provided the inputs and stimuli necessary to the establishment of this collaborative effort.

Lastly, this book is published thanks to the precious editorial help of Marion Jahan.