Chapter 2
End-to-End, Net Neutrality and Human Rights

Luca Belli

2.1 Introduction

The network neutrality (NN) debate focuses on the effects that Internet Traffic Management (ITM) practices, implemented by network operators, may deploy on Internet users' rights and, particularly, on their capability to freely seek, receive and impart information and ideas. Certain ITM techniques are indeed aimed at discriminating against specific content, applications and services and, therefore, have the potential to substantially interfere with the end-user's Internet experience. Over the past 15 years,[1] NN discussions have been scrutinising the extent to which ITM techniques may be deemed as reasonable, trying to find a delicate balance between the interests of the operators, which have the technical possibility to manage Internet traffic; the interests of the Content and Application Providers (CAPs) that rely on non-discriminatory Internet connectivity in order compete on a level playing field; and the interests of Internet users, who rely on non-discriminatory Internet connectivity in order to fully enjoy their fundamental rights while, as customers, have a legitimate expectations to enjoy the quality levels for which they pay.

As I will briefly argue in this paper, the very design of the original Internet architecture was not only instrumental to allow thousands of heterogeneous networks to interoperate, but played also a key role allowing end-users to fully enjoy freedom of expression and innovation. Indeed, in the online environment, freedom to receive and impart information and ideas is directly reflected on users' capability to freely access and share content, applications and services, using the device of their choice, without being unduly influenced by discriminatory delivery of Internet traffic.

[1] Even before the creation of the expression "network neutrality", by Wu (2003), the substance of the debate had already been explored by several scholars starting from the late 1990s. See *e.g.* Marsden (1999), Cooper (2000), Lemley and Lessig (2000).

L. Belli (✉)
Fundação Getúlio Vargas Law School, Rio de Janeiro, Brazil
e-mail: luca.belli@fgv.br

L. Belli, P. De Filippi (eds.), *Net Neutrality Compendium*,
DOI 10.1007/978-3-319-26425-7_2

Such user capability has been unleashed by the originally open design of the Internet, which substantially differed from the traditionally closed and centralised architecture of telecommunications networks. Differently from previous communication systems, which were based on the operators' capability to define the networks' purpose, the Internet has been designed as a decentralised, general-purpose network. This open and decentralised architecture did not allow operators to discriminate against specific applications, services or content. The Internet has been conceived as an agnostic platform with regard to the content that may be conveyed and the purpose for which it can be used, thus allowing end-users to freely decide how to utilise their applications. Such fundamental features have empowered individuals with the capability to freely communicate and innovate, thus realising the promise of the Universal Declaration of Human Rights: "Everyone shall have the right to freedom of expression; this right shall include the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers and without interference."

In this paper, I argue that the safeguard of the NN principle plays an instrumental role in maintaining the aforementioned open and decentralised architecture. NN is commonly referred as the principle according to which all electronic communication networks shall carry data in a non-discriminatory fashion regardless of their content, the type of application, the identity of their sender and recipient or the type of device used.[2] Hence, this paper stresses that NN policies are key to facilitate the full enjoyment of Internet users' freedom of expression, as well as other fundamental rights. Simultaneously, this paper highlights that ITM practices consisting in blocking, filtering, throttling or prioritising specific data flows, are in contrast with the NN principle and have the potential to unduly interfere with end-users' enjoyment of their fundamental rights as well as to jeopardise the Internet's fundamentally open architecture. It is important to note that, as freedom of expression, NN is not an absolute principle and limitations should be foreseen. However, in light of the instrumental role played by NN to safeguard Internet users' rights, limitations to this principle should be allowed only when necessary and proportionate to the achievement of a legitimate aim.

After providing a brief overview of the Internet's end-to-end architecture (Sect. 2.2), the article will categorise some commonly used ITM techniques, stressing the impact that such techniques may have on Internet users' fundamental rights (Sect. 2.3). Lastly, the article will analyse the emergence of NN policies and regulations protecting the NN principle (Sect. 2.4), and will provide some policy suggestions aimed at fostering a human rights approach to this all-important topic.

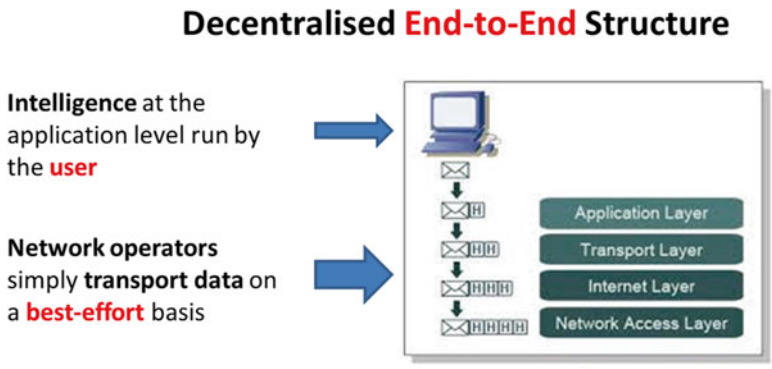
2.2 From End-to-End to Centralisation

The original Internet architecture was grounded on the end-to-end (E2E) design principle (Saltzer et al. 1984; Carpenter 1996). The E2E principle essentially affirmed that the various functions for which the Internet might be used "*can*

[2] See United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information 2011, para. 5; DCNN Model Framework on Network Neutrality, para 1.

completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible" (Saltzer et al. 1984). The E2E system design established an open, non-discriminatory and general-purpose network, decentralising the definition and implementation of the network functions—*i.e.* the Internet's "intelligence"—at the end-user level. Although this design choice was made for efficiency purposes, its collateral effect has been to unbridle end-users' freedom of expression and innovation in an unprecedented way.

The E2E principle may be considered as one of the underlying arguments in favour of NN. Indeed, the E2E argument ascribes to users the "responsibility for the integrity of communication",[3] assuming that operators manage internet traffic in an essentially non-discriminatory fashion and delegating the detection and resolution of potential data-delivery problems to the applications run at the edges of the communication network. As such, according to the E2E principle, end-users play an active role, running and creating applications at the "endpoints" of the network whilst the communications network are considered as passive infrastructure, tasked with the mere transportation of data packets[4] on a best-effort[5] basis.



Source: Belli 2015a

As famously stated by the Internet Engineering Task Force, "*the goal* [of the Internet] *is connectivity, the tool is the Internet Protocol, and the intelligence is end*

[3] According to the Request for Comments 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 Carpenter (1996).

[4] In an electronic communications network, information is fragmented into so-called data packets. The data packet is the basic a unit of digital information that travels along a given network path on 'packet-switched' networks.

[5] The concept of "best effort delivery […] refers to the way in which data is conveyed over the Internet – namely operators transmitting data streams to convey them from their point of departure to their destination, with no guarantee on performance but only an obligation of best endeavor". See ARCEP (2012), p. 16.

to end rather than hidden in the network" (Carpenter 1996). Conspicuously, by requiring that functionalities be implemented at the network's endpoints, when possible, and at the network level only when necessary, the E2E principle places the end-users, rather than the operator, in control of their Internet experience. Such decentralised system has proven to be essential to foster and maintain Internet openness, removing discriminatory barriers that may hinder the free flow of information and innovation. However, since the early 2000s, the Internet ecosystem has started to manifest some early sign of centralisation, triggered by the increasing use of discriminatory ITM techniques. In this regard, discussions regarding the need for NN policies have been sparked by the fear that network operators' ITM capabilities may allow them to act as chokepoints (Cooper 2000). Indeed, operators may be tempted to use discriminatory ITM measures to block or downgrade the content, applications and services that compete with their own offerings—or with the offerings of their commercial partners—thus hampering competition, jeopardising end-users' freedom of expression and, ultimately, "putting an end" to the end-to-end architecture (Lemley and Lessig 2000). On the contrary, the limitation of network operators' capacity to discriminate against specific content, applications and services to what is necessary and proportionate to the achievement of a legitimate aim, has been considered as essential to minimise possible side effects of ITM practices, thus preserving an open and user-empowering Internet (FCC 2010; BEREC 2012c).

NN has been first conceptualised as a "network design principle" whereby 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 (Wu 2003). However, NN has rapidly evolved into a policy principle or even a "policy priority",[6] due to the increasing realisation of the impact that ITM techniques may have on free competition as well as on end-users rights (BEREC 2012a; FCC 2015). NN policies are aimed at preserving an open and decentralised Internet architecture, avoiding possible negative impacts of ITM practices on the free flow of information. Indeed, non-discriminatory traffic management is supposed to facilitate a virtuous cycle of innovation (FCC 2010; Williamson et al. 2011), reinvigorating end-users' freedom of expression and unleashing their capacity to share new applications and services (Lee and Wu 2009; BEREC 2012a; Belli and Van Bergen 2013). However, it is important to note that, although ITM measures are expression of the operators' power to act as centralised Internet points of control, the use of ITM techniques should not be considered as something illegitimate *per se*. On the contrary, although extensive use of ITM favours the centralisation of network control in the hands of operators, it must be noted that some forms of traffic management are essential to preserving well-functioning networks. As an instance, the use of ITM techniques to block the expansion of malware

[6] See BEREC (2012b). Furthermore, since 2010, the Council of Europe members have explicitly declared their intention to preserve "the interoperability of the Internet as well as its end-to-end nature" arguing that "[t]hese principles should guide all stakeholders in their decisions related to Internet governance. [and t]here 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 Council of Europe (2010).

clearly serves the legitimate interests of the end-users, preserving the integrity and security of the networks. On the other hand, some ITM techniques may be used for purposes that can harm end-users rights. For instance, blocking or throttling applications provided by the operators' competitors is undeniably an unreasonable and illegitimate practice, because the only rationale of such discriminatory treatment is to avoid free competition. The section below provides some further elements aimed at categorising the purposes of existing ITM practices and clarifying their possible effects on Internet users' rights.

2.3 Internet Traffic Management and Mismanagement

As noted above the original Internet architecture was based on the "best effort delivery" model for transmission of data packets, whereby operators convey Internet traffic in a non-discriminatory fashion without any guarantee of quality or obligation over the result. The non-discriminatory traffic management enabled by the best effort model has proved to be particularly beneficial, "defining low barriers to entry on the open platform of the Internet, which has provided particularly fertile ground for new content and applications to develop" (BEREC 2012a). However, it must be noted that, even within a best-effort paradigm, Internet traffic is continuously processed both by the end-users' terminal machines and by the network genitive operators equipment. On the one hand, end-users' machines constantly perform congestion control, increasing or decreasing the data transmission rate, depending on network congestion.[7] On the other hand, operators commonly implement ITM practices to mitigate the effect of network congestion, protect networks' security and integrity and optimise available network resources. To do so, operators monitor their networks to understand the traffic behaviour and implement technical means that target the traffic sent or received by end users. The ITM techniques implemented by operators may be protocol-agnostic or protocol-specific. The former do not discriminate against specific classes of applications while the latter do. As an instance, "First-in, first-out" (FIFO) routing technique is fully protocol-agnostic while blocking or prioritising Voice over IP (VoIP) applications like Skype is quintessentially protocol-specific. Furthermore, ITM practice may also be application-specific thus targeting specific content or a particular application or service, rather than a class of applications.

Application-specific techniques may raise net neutrality concerns because they explicitly aim at managing Internet traffic in a discriminatory fashion, by blocking, filtering, throttling or prioritising specific data flows, thus impeding the end-user from having full control of his/her Internet experience. As such, application-specific mea-

[7] It is important to note that "there are two types of congestion that generally present themselves in a network. The first general type of congestion is regularly occurring and is the result of gradually increasing traffic levels up to a point where typical usage peaks cause congestion on a regular basis. […]The second general type of congestion is unpredictable congestion, which can occur for a wide range of reasons. One example may be due to current events, where users may be all rushing to access specific content at the exact same time […]." See Bastian et al. (2010).

sures may result in restrictions to access legitimate content and/or applications and may be exploited by operators to favour the CAPs with which they vertically integrate or disfavour their competitors (BEREC 2012a; FCC 2015). At the European level, for instance, an investigation led in 2012 by BEREC (the Body of European Regulators of Electronic Communications) and the European Commission highlighted the existence of a wide array of traffic management practices resulting in undue restrictions (BEREC 2012a). Therefore, applications specific measures should be considered as contrary to net neutrality when they are not necessary and proportional to the achievement of a legitimate purpose (BEREC 2012c; Belli and van Bergen 2013).

It is important to note that network operators may implement ITM techniques at different levels of their infrastructure (*e.g.* access lines, transit lines, switching nodes, etc.) and protocol-specific or application-specific ITM may have different purposes. Particularly they may be aimed at:

- Blocking access to specific content, applications and services. Such practice may be put in place in order to comply with national legislation, may be used for security purposes *e.g.* blocking ports to prevent spam or other harmful traffic, but may be also implemented to inhibit competing services. To this latter extent, some network operators have been inhibiting protocols exploited by competing services, such as VoIP, in order to preserve their business model. Blocking practices prevent communications without inspecting data packets, whereas filtering techniques imply that the content of communications must be inspected before being blocked.
- Filtering specific data packets. This practice aims at granularly analysing Internet traffic to identify specific content and apply a particular treatment, such as blocking, throttling or prioritisation. Hence, this technique requires installing content inspection equipment so that Internet traffic is analysed when passing through the filtering equipment. This technique can be used to preserve network security and integrity, for instance filtering out spam or limiting the effect of malicious attacks, but may also be used for censorship purposes and has the potential to jeopardise the privacy of end-users' communications.
- Bandwidth throttling. In this case, the operator downgrades specific type of Internet traffic (*e.g.* all video traffic) or specific bandwidth-greedy applications (*e.g.* peer-to-peer) in order to limit the congestion they generate. However, bandwidth throttling may be also exploited to reduce the quality of competing applications. Such technique may be applied temporary and exceptionally but can be also applied on a general basis, to discriminate against a specific type of traffic or applications, despite the existence of congestion.
- Traffic prioritisation. Differently from bandwidth throttling, this kind of technique gives, preferential treatment to specific types of traffic *e.g.* by prioritising time-sensitive applications, such as VoIP, or to guarantee quality of service of specific services. This latter case may happen when operators implement pay-for-priority schemes, allowing specific CAPs to purchase preferential treatment, or when operators deploy specialised services (such as IPTV or e-health services) with no separation from Internet access services. It is important to note that the quality of the non-prioritised applications—or of the general Internet

access service, in case of non-separated specialised services—may be degraded, due to sharing resources.

As stated above, protocol-specific and application-specific ITMs can be considered as legitimate exceptions to the NN principle only when necessary, proportional to a legitimate purpose. Although blocking practices have been criticised for their negative side-effects (SSAC 2012; BITAG 2013), such techniques may be justified by court orders aimed at impeding access to material deemed as illegal by national legislations, in conformity with human rights norms and international law. However, blocking may be also used to impede access to specific applications, such as instant messaging, VoIP or Video on Demand (VoD), that may compete with traditional services offered by the operators, such as text messaging, voice calls or TV (BEREC 2012a; BITAG 2013). Therefore, operators may have a concrete incentive to block access to competing services, particularly when operators vertically integrate with CAPs offering analogue services. Likewise, operators may temporarily and exceptionally throttle bandwidth-greedy applications—or prioritise time-sensitive applications—in order to handle congestion but the same measures may be used in order to downgrade competing services or prioritise the applications provided by commercial partners (BEREC 2012a; FCC 2015). For instance, in 2005 the U.S. Federal Communication Commission (FCC) found the Internet access provider Madison River Communications unduly blocking the Voice over IP (VoIP) service Vonage (FCC 2005a) whilst, in 2008, the FCC found the operator Comcast unduly throttling the peer-to-peer application BitTorrent (FCC 2008).

As it has been noted above, besides undermining free competition, the unrestricted use of such application-specific techniques may jeopardise the effective exercise of fundamental rights and freedoms such as freedom of expression or privacy. On the one hand, by blocking or downgrading legitimate applications and services, operators exercise an undue interference in users' freedom to seek, receive and impart information and ideas. It is important to stress that such risks are not merely theoretical or confined to authoritarian regimes. As an example, in 2012, four British operators blocked access to the TOR-project website, a website offering privacy-enhancing technologies (TOR Project 2012), while another mobile operator blocked access to the website of the advocacy group La Quadrature du Net (Cappuccini and Craggs 2012). Both cases highlight the very tangible threats that unregulated blocking may determine on freedom of communication and information. On the other hand, it must be noted that the use of pervasive inspection techniques—such as Deep Packet Inspection (DPI)—for filtering purposes may determine nefarious consequences on users' fundamental right to privacy (EDPS 2011, 2013). DPI technologies are indeed able to examine the content of the data packets conveyed through an electronic network and, based on the result of the analysis, can apply a discriminatory treatment defined by the operator. DPI technologies are commonly used to monitor and manage both fixed and wireless networks for many purposes, amongst which the prevention of online pornography and copyright infringement. 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.[8] However, due to the processing of high quantity of personal data, the unnecessary and disproportioned use of such invasive techniques may severely compromise the privacy of Internet users' electronic communications (EDPS 2011, 2013).

In light of the above considerations, it seems essential to stress that ITM measures should not be considered as a mere technical issue and the potential implications of such practices on Internet users' rights should be carefully assessed. On the one hand, the implementation of protocol specific—or application-specific—ITM techniques must be legitimate, proportional and necessary[9] while, on the other hand, the use of non-discriminatory ITM promoted by the NN principle should be preferred and fostered due to the social benefits that it can determine (Van Schewick 2010; BEREC 2012a).

2.4 From End-to-End to the Rule of Law

After having been suggested by several U.S. academics (*e.g.* Cooper 2000; Lemley and Lessig 2000; Wu 2003), the risks of ITM practices have been concretely demonstrated by a number of cases around the world. Some violations may be patent and clearly identifiable, as the abovementioned Madison River case (FCC 2005a), in which the American ISP Madison River Communications was found guilty of using port blocking to prevent its subscribers from using VoIP services offered by Vonage, in order to protect its telephone service business. Madison River deliberately impeded access to a VoIP service perceived as competing, disregarding end-users' freedom to choose a perfectly legal VoIP application as well as their freedom to communicate with such perfectly legal service. However, not all violations may have such a clear-cut nature and may be difficult to identify or prove in the lack of an appropriate framework. Due to the negative effects that certain ITM measures may have on the free market as well as to the full enjoyment of Internet users' rights, many regulators and policy-makers consider the protection of the NN principle as a true policy priority (BEREC 2012b). In this regard, several national systems already protect NN by means of legislation or through self/co/regulatory frameworks.

The first regulatory approach to NN was adopted by the U.S. Federal Communications Commission through Policy Statement (FCC 2005b), establishing four basic principles, according to which Internet users should be entitled to:

- access the lawful Internet content of their choice;

[8] See UNESCO (2012).

[9] 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.

- 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.

This approach to NN nurtured the European policy-making efforts, both at the EU level, during the 2009 revision of the Telecoms Package, and at the Council of Europe level, with the adoption of the Committee of Ministers' Declaration on Network Neutrality, in 2010. On the one hand, the Universal Service Directive affirmed that European end-users "*should be able to decide what content they want to send and receive, and which services, applications, hard ware and software they want to use for such purposes, without prejudice to the need to preserve the integrity and security of networks and services*" while leaving to market competition the task to "*provide users with a wide choice of content, applications and services*" and delegating to national regulators the task to "*promote users' ability to access and distribute information and to run applications and services of their choice.*"[10] On the other hand, recognising the possibility that "*users' right to access and distribute information online and the development of new tools and services might be adversely affected by non-transparent traffic management*" and the instrumental role played by NN in order to foster the full enjoyment of fundamental rights, the Council of Europe's Committee of Ministers declared "*its commitment to the principle of network neutrality*".[11] further specifying that "*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*".[12]

Both the original FCC and EU approaches were grounded on competition and no-blocking rules, to which EU policymakers added transparency obligations[13]—taking inspiration from the Norwegian Principles on Internet Neutrality[14]—as well as the national regulators' power to impose "*minimum quality of service requirements*".[15] On both sides of the Atlantic, the rationale was to avoid hard regulation on ITM practices and delegate to free competition and informed consumer choice the task to avoid discriminatory treatments. However, it should be noted that, in order to be both market efficient and human-right-efficient, competition law principles and transparency obligations presuppose an ideal situation. In such ideal situation, competition would guarantee that all information and ideas can be freely conveyed without discrimination, while rational consumers have both the time and the technical skills necessary to analyse the ITM information contained in Internet-access-service contracts and, subsequently, "vote with their feet", abandoning

[10] See Directive 2009/136/EC, recital 28.

[11] See Council of Europe (2010), para. 9.

[12] See *ibid.*, para. 4.

[13] See Directive 2009/136/EC, recital 23.

[14] See Annex 1.

[15] See Directive 2009/136/EC, recital 34 and art 22(3).

those network operators that unduly discriminate against specific content, applications. Such scenario seems overconfident for several reasons.

On the one hand, the aforementioned scenario relies on the assumption that all end-users have the technical background necessary to understand that eventual problems to access or use a given application may be due to the implementation of discriminatory ITM techniques rather than supposing the malfunctioning of the application (*i.e.* the so-called "the-application-doesn't-work situation"). Furthermore, the competition-based approach overestimates the market capability to distribute efficiently speech. Indeed, not all information has the same value. Due to the profitability of content, services and applications, network operators that vertically integrate with CAPs have a considerable incentive to "*use the architecture of the Internet to nudge their customers into planned communities of consumerist experience, to shelter end users into a world that combines everyday activities of communication seamlessly with consumption and entertainment* [eventually pushing] *consumers back into their pre-Internet roles as relatively passive recipients of mass media content*" (Balkin 2004). It is important to note that some information and ideas may be more profitable than other and, therefore, if information flows were to be determined primarily—or even solely—by profit maximisation criteria, there could be a serious risk that inconvenient and non-profitable information would be *de facto* excluded (Belli and van Bergen 2013).

On the other hand such assumption underestimate the fact that, even in a competitive market, the majority of the operators—or, potentially, all operators—may discriminate against specific content, applications and services, thus making it irrelevant to switch from one operator to the other. In this regard, it seems important to mention that the joint investigation led by BEREC and the European Commission found that in Europe—which is usually considered as a quite competitive market—at least 36 % of mobile Internet users and 25 % of all European Internet users were affected by some type of restrictions, particularly involving blocking and throttling practices (BEREC 2012a). Lastly, the competition-based approach fails to consider the fact that, the Internet ecosystem is composed of an interconnection of networks and, therefore, discriminatory practices implemented by network operator A—*e.g.* blocking a specific application—may also affect the capability of other operators' customers to freely communicate. Indeed, the customers of network B or C would be unable to communicate with the users of network A, *e.g.* using the blocked application, even if traffic restrictions are implemented only within network A. Hence, in light of the abovementioned considerations, it is important to stress that although competition and transparency are essential in order to guarantee NN, they are not sufficient *per se*.

2.5 Conclusion: Towards a Human Rights Approach

As highlighted above, NN focuses on preserving a distributed and user-empowering Internet architecture, allowing individuals to fully enjoy their freedom of expression, imparting and receiving any lawful content, services or application, using any legal device. NN aims at strengthening the fundamental features of the original

Internet environment, such as end-to-end architecture and best-effort delivery, in order to safeguard the Internet's user-empowering capacity. As such, the non-discriminatory treatment mandated by the NN principle seems to be instrumental not only to facilitate the full enjoyment of fundamental rights but also to safeguard the "openness and fairness" as well as the "decentralized control, edge-user empowerment and sharing of resources" that represent the very "scope of the Internet," as recognised by the Internet technical community itself (Alvestrand 2004).

In order to preserve an open and user-centric Internet, the implementation of ITM techniques capable of shifting the control of the Internet experience from the user to the operator should be allowed exclusively when necessary and proportionate to the achievement of a legitimate aim. Particularly, the use of such measures should be justified on grounds of verifiable technical necessity or to address transient network management problems which cannot otherwise be addressed, or should be required by court orders and national laws in conformity with international human rights norms and legislation. As argued above, discriminatory ITM practices have the potential to jeopardise end-users fundamental rights such as privacy and freedom of expression. Authoritative jurisprudence has stressed that freedom of expression "*applies not only to the content of information but also to the means of dissemination since any restriction imposed to the [means] necessarily interfere with the right to receive and impart information*" (ECtHR 1990). Indeed, from a European perspective, discriminatory traffic management can be seen as an interference with freedom of expression, which "*applies not only to the content of information but also to the means of dissemination*" (ECtHR 2012). Likewise, the Inter-American Court of Human Rights (IACHR) has explicitly argued that "*equity must regulate the flow of information*", establishing the state obligation to "*extend equity rules, to the greatest possible extent, to the participation in the public debate of different types of information, fostering informative pluralism*" (IACHR 2008, 2011).

It is important to note that, in the absence of any policies or regulations aimed at promoting NN and avoiding the possible negative impact of ITM techniques, the only entities able to define the contours of ITM are the operators themselves. Such entities frequently integrate with CAPs, thus having a substantial economic incentive not to be neutral, thus favouring commercial partners and disfavouring competitors. Hence, it seems necessary to foster the definition of "rules of the road" for operators, aimed at guaranteeing the full enjoyment of end-users' rights while avoiding the potentially nefarious effects of discriminatory traffic management. However, it seems important to note that, as freedom of expression, the NN principle should not be considered as absolute and exceptions to the NN should be allowed and clearly defined, in order to allow so-called "reasonable traffic management", while fostering legal certainty. To this latter extent, policymakers should promote the elaboration of regulatory approaches—or co-regulatory approaches, where the definition and implementation of NN principles or codes of conduct is overseen by regulators—aimed at clearly defining the limits of ITM practices, so that end-users rights are fully respected.

2.6 Annex 1: Norwegian Principles on Internet Neutrality

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 (a) send and receive content of their choice; (b) use services and run applications of their choice; (c) 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.[16]

2.7 Annex 2: Dutch Legal Provision on Network Neutrality

Article 7.4a, Telecommunications Act (unofficial translation[17])

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:

   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.

[16] 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.

[17] 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/.

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 communications networks.

2.8 Annex 3: Slovenian Legal Provisions on Network Neutrality

Article 203, Electronic Communications Act (unofficial translation[18])

(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.
(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 of:

[18] See Slovenian Electronic Communications Act, available at http://www.uradni-list.si/_pdf/2012/Ur/u2012109.pdf#!/u2012109-pdf.

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. decisions 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 via internet access services.
(6) The Agency can issue a general act to implement the provisions of the third, fourth and fifth paragraphs of this Article.

2.9 Annex 4: Brazilian Legal Provisions on Network Neutrality

Article 9, Law No. 12 .965, 23 April 2014 (unofficial translation[19])

The party responsible for the transmission, switching or routing has the duty to process, on an isonomic basis, any data packages, regardless of content, origin and destination, service, terminal or application.

§1° The discrimination or degradation of traffic shall be regulated in accordance with the private attributions granted to the President by means of Item IV of art. 84 of the Federal Constitution, aimed at the full application of this Law, upon consultation with the Internet Steering Committee and the National Telecommunications Agency, and can only result from:

I—technical requirements essential to the adequate provision of services and applications;
and II—prioritization of emergency services.

§2° In the happening of discrimination or degradation of traffic provided in §1°, the responsible entity mentioned in Art. 9 o must:

I—abstain from causing damages to users, as set forth in art. 927 of Law n° 10.406, January 10th, 2002 the Civil Code;
II—act with proportionality, transparency and isonomy;

[19] See Lei N° 12.965, de 23 de abril de 2014, also known as Marco Civil da Internet no Brasil. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

III—provide, in an advanced notice, in a transparent, clear and sufficiently descriptive manner, to its users, the traffic management and mitigation practices adopted, including those related to network security;
and IV—offer services in non-discriminatory commercial conditions and refrain from anti-competition practices.

§3° When providing internet connectivity, free or at a cost, as well as, in the transmission, switching or routing, it is prohibited to block, monitor, filter or analyze the content of data packets, in compliance with this article.

References

Alvestrand, H. T. (2004, October). A Mission Statement for the IETF. Request for Comments: 3935. BCP: 95. https://www.ietf.org/rfc/rfc3935.txt

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

Balkin, J. M. (2004). Digital speech and democratic culture: A theory of freedom of expression for the information society. *New York University Law Review, 79*(1).

Bastian, C., Klieber, T., Livingood, J., Mills, J., & Woundy, R. (2010, December). *An ISP Congestion Management System. RFC 6057*. https://tools.ietf.org/html/rfc6057#page-9

Belli, L. (2015, June 8) *From Internet Standards to Regulatory Standards? A Net Neutrality Experiment*. Presented to Conferência Internacional sobre a Elaboração de Regras de Neutralidade de Rede, FGV Rio de Janeiro. https://www.youtube.com/watch?v=_W_jV14Xc-4

Belli, L., & van Bergen, M. (2013). *Protecting Human Rights through Network Neutrality: Furthering Internet Users' Interest, Modernising Human Rights and Safeguarding the Open Internet*. Council of Europe. CDMSI(2013)Misc19.

BEREC. (2012a, May 29). *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. BoR (12) 30. https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf

BEREC. (2012b, November 27). *Overview of BEREC's approach to net neutrality*. BoR (12) 140 http://berec.europa.eu/files/document_register_store/2012/12/BoR_%2812%29_140_Overview+of+BEREC+approach+to+NN_2012.11.27.pdf

BEREC. (2012c, December 3). *Summary of BEREC positions on net neutrality*. BoR (12) 146. http://berec.europa.eu/files/document_register_store/2012/12/BoR_%2812%29_146_Summary_of_BEREC_positions_on_net_neutrality2.pdf

BITAG. (2013, August). *Port Blocking. A Broadband Internet Technical Advisory Group Technical Working Group Report*. http://www.bitag.org/documents/Port-Blocking.pdf

Cappuccini, A., & Craggs, G. (2012, February 15). Orange UK blocking La Quadrature du Net. Open Rights Group. https://www.openrightsgroup.org/blog/2012/orange-uk-blocking-la-quadrature-du-net

Carpenter, B. (1996). *Architectural Principles of the Internet. Request for Comments: 1958*. https://www.ietf.org/rfc/rfc1958.txt

Cooper, M. (2000). *Open Access to the Broadband Internet: Technical and Economic Discrimination in Closed, Proprietary Networks*, 71 U. Colo. L. Rev. 1011.

Council of Europe. (2010). *Declaration of the Committee of Ministers on Network Neutrality*. Adopted by the Committee of Ministers on 29 September 2010 at the 1094th meeting of the Ministers' Deputies. https://wcd.coe.int/ViewDoc.jsp?id=1678287&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

DCNN. (2013). *Model Framework on Network Neutrality*. Presented at meeting of the Dynamic Coalition on Network Neutrality held during the 8th Internet Governance Forum. Bali 2013. http://www.networkneutrality.info/sources.html

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

ECtHR. (1990, May 22). Autronic AG v. Switzerland, 22 May 1990. Application no. 12726/87. http://hudoc.echr.coe.int/eng?i=001-57630

ECtHR. (2012, December 18). Case of Ahmet Yıldırım v. Turkey. Application no. 3111/10. http://hudoc.echr.coe.int/fre?i=001-115705

EDPS. (2011, October 7). *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

EDPS. (2013, November 14). *Opinion of the Europe on Data Protection Supervisor on the Proposal for a Regulation of the Europe on Parliament and of the Council laying down measures concerning the Europe an single market for electronic communications and to achieve a Connected Continent*.

FCC. (2005a). Madison River Communications, LLC and affiliated companies, Acct. No. FRN: 0004334082. https://transition.fcc.gov/eb/Orders/2005/DA-05-543A2.html

FCC. (2005b). Policy Statement. 20 FCC Rcd 14986, 14987–88. Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf

FCC. (2008, August 1). *Commission Orders Comcast to End Discriminatory Network Management Practices*. News Media Information 202/418-0500. https://apps.fcc.gov/edocs_public/attachmatch/DOC-284286A1.pdf

FCC. (2010). *Preserving the Open Internet*, GN Docket No. 09-191, WC Docket No. 07-52, Report and Order, 25 FCC Rcd 17905, 17911.

FCC. (2015). *Report and Order on Remand, Declaratory Ruling, and Order on the Matter of Protecting and Promoting the Open Internet*. GN Docket No. 14-28.

IACHR. (2008). *Case of Kimel v. Argentina. Merits, Reparations and Costs*. Judgment of May 2, 2008. Series C No. 177. Para. 57.

IACHR. (2011). *Case of Fontevecchia y D'Amico v. Argentina. Merits, Reparations and Costs*. Judgment of November 29, 2011. Series C No. 238. Para. 45.

Lee, R. S., & Wu, T. (2009). Subsidizing creativity through network design: zero pricing and net neutrality. *Journal of Economic Perspectives, 23*(3).

Lemley, M., & Lessig, L. (2000, October 1). The end of end-to-end: preserving the architecture of the Internet in the broadband era. *UCLA Law Review, 48*, 925, 2001, available at: http://ssrn.com/abstract=247737

Marsden, C. (1999). *Pluralism in the multi-channel market. Suggestions for regulatory scrutiny.* Council of Europe MM-S-PL(1999)012 http://www.coe.int/t/dghl/standardsetting/media/Doc/MM-S-PL(1999)012_en.asp

Saltzer, J. H., Reed, D. P., & Clark, D. D. (1984). End-to-end arguments in system design. *ACM Transactions on Computer Systems,* (2). http://web.mit.edu/saltzer/www/publications/endtoend/endtoend.pdf

SSAC. (2012, October 9). *SSAC Advisory on Impacts of Content Blocking via the Domain Name System*. SAC 056. https://www.icann.org/en/system/files/files/sac-056-en.pdf

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

UNESCO. (2012). *Liberté de connexion Liberté d'expression – Ecologie dynamique des lois et règlements qui façonnent l'Internet*. http://unesdoc.unesco.org/images/0021/002160/216029f.pdf

United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the

African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information. (2011). *Joint Declaration on Freedom of Expression and the Internet*.

Van Schewick, B. (2010). *Internet architecture and innovation*. MIT Press.

Williamson, B., Black, D., & Punton, T. (2011, October). *The open internet – A platform for growth*. A report for the BBC, Blinkbox, Channel 4, Skype and Yahoo!

Wu, T. (2003). Network neutrality, broadband discrimination. *Journal of Telecommunications and High Technology Law, 2*.

http://www.springer.com/978-3-319-26424-0

Net Neutrality Compendium
Human Rights, Free Competition and the Future of the Internet
Belli, L.; De Filippi, P. (Eds.)
2016, XIX, 300 p. 5 illus., Hardcover
ISBN: 978-3-319-26424-0