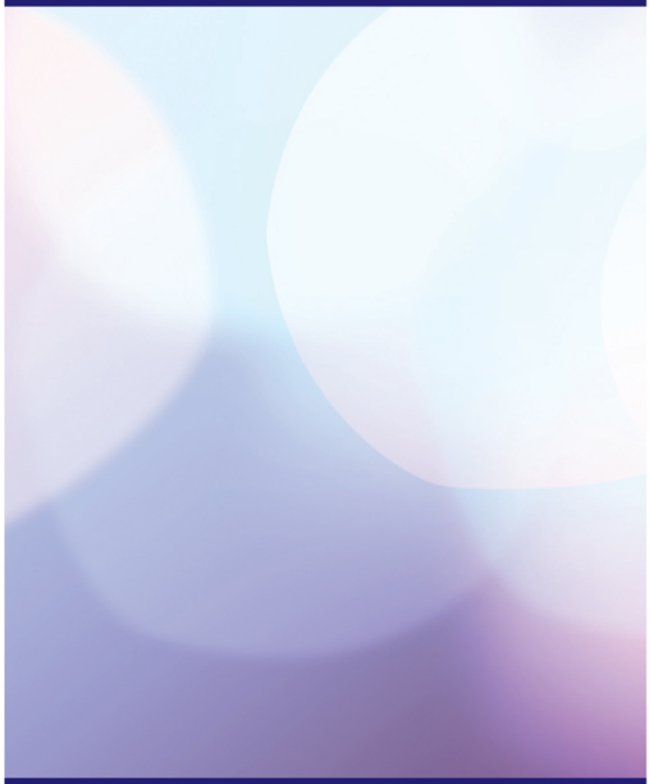
analysys mason



www.analysysmason.com

Final public report for BEREC

Study on net-neutrality regulation

18 September 2017

James Allen, Andrew Daly, J. Scott Marcus, David de Antonio Monte, Robert Woolfson

Ref: 2009152-254

Contents

Analysys Mason Limited
North West Wing, Bush House
Aldwych
London WC2B 4PJ
UK
Tel: +44 (0)20 7395 9000
london@analysysmason.com
www.analysysmason.com
Registered in England No. 5177472

1 Executive summary

1.1 Background and purpose of the work

BEREC commissioned Analysys Mason and Scott Marcus to study the approach taken by national regulatory authorities (NRAs) in selected non-European benchmark countries to address net-neutrality issues. The benchmark countries are:

- Chile (SUBTEL)
- India (TRAI)
- USA (Federal Communications Commission (FCC)).

The study aims to contribute to an informed public debate and constitute a valuable source of practical information for European NRAs and BEREC while they are implementing EU regulation 2015/2120.[1] The study also aims to help BEREC and European NRAs to define their options for addressing net-neutrality issues and identify the requirements and challenges they may face in future. It should be noted that the study does not include comparisons between the benchmark countries and the European regulatory framework.

1.2 Overview of approach to tackling net neutrality in each country

Each of the NRAs is tackling net neutrality[2] within a slightly different context:

Chile (SUBTEL) Chile was the first country in the world to define a net-neutrality law, which sets out a principled approach for SUBTEL to regulate the industry. After some initial high-profile violations involving zero rating, net neutrality in Chile appears to be progressing without further incident. SUBTEL is currently focusing on gathering quality-of-service (QoS) data and transparency; monitoring of net-neutrality-specific practices is limited to qualitative information provided by Internet service providers (ISPs).

India (TRAI) India is tackling net neutrality on a more incremental basis (i.e. one issue at a time), having defined a regulation which refers only to the specific issue of differential tariffs (to address the issue of zero rating). TRAI recently closed a consultation on the wider issues associated with net neutrality,[3] but at the time of writing no further decision or regulation had been issued. TRAI operates an "Analytics Portal" which collects data on QoS for mobile services, but no net-neutrality-specific data gathering takes place.

1 The regulation is already complemented by implementation guidelines from BEREC.

2 It should be noted that we are not using an absolute definition of net neutrality, but rather the general principle, as each country has a different version that it is looking at.

3 The consultation closed on 26 April 2017. TRAI has also previously consulted on issues associated with over-the-top (OTT) services, which included a chapter on net neutrality. This previous consultation closed on 8 May 2015.

USA (FCC)

Similar to Chile, the USA also considered the issue of net neutrality at an early stage, by defining the Open Internet Order in 2010 (subsequently updated in 2015). Recent changes within the regulator FCC mean that the future of net-neutrality regulation in the USA is highly uncertain. However, historical developments in the USA are highly informative, as a wide range of practices were identified which were found to violate net-neutrality principles. Monitoring in the USA places heavy reliance on a complaints system, as there is no net-neutrality-specific monitoring in place. The FCC operates a comprehensive QoS measurement programme.

Figure 1 provides an overview of the approach that NRAs in Chile, India and the USA have taken to net neutrality.

Figure 1: Overview of net-neutrality issues in benchmark countries [Source: Analysys Mason, 2017]

Aspect of net neutrality	Chile	India	USA
History of practices considered under net neutrality	Zero rating of social media sites	Zero rating of certain apps and website	Wide range of issues, including blocking, throttling, interconnection capacity and zero rating
Transparency by ISPs	Detailed quarterly reporting requirements laid down in regulation, with quantitative QoS reporting and qualitative traffic-management reporting	Quarterly performance-monitoring reporting by ISPs	Detailed transparency requirements issued by the FCC, with quantitative QoS data gathered via a hardware-based measurement platform. Qualitative traffic management reporting
Monitoring and supervision by NRA	SUBTEL monitors QoS reporting by ISPs	There is currently no net-neutral-specific monitoring or supervision undertaken by TRAI Complaints can be made to TRAI via its portal, or via the Consumer Redressal Forum	No active monitoring of the transparency reporting by ISPs An established complaint system allowing any party to signal a potential violation to the FCC for review
Legal mechanisms for enforcement by NRA	Net-neutrality law is the basis of enforcement. SUBTEL can issue fines for violations	TRAI can enforce non-discriminatory tariffs, and issue fines	The FCC's Enforcement Bureau can enforce net neutrality on the basis of the Open Internet Order of 2015. The FCC can issue fines
Regular reporting by NRA	Twice-yearly 'state of market' reports include QoS-related data	QoS metrics are available on TRAI's Analytics Portal	Annual reporting of QoS metrics

1.3 Case studies of monitoring tools and techniques

We have prepared four case studies from the benchmark countries, which are summarised below:

- Adkintun, Chile
- Sistema de Transferencia de Información (STI), Chile
- Netalyzr, USA
- Measuring Broadband America programme, USA.

Although none of the benchmark countries has tools and techniques which have been specifically designed for monitoring non-net-neutral practices, the case studies illustrate interesting principles or monitoring approaches which may be of use to European NRAs as they develop their approach for addressing net neutrality.

Case study 1: Adkintun, Chile

The Adkintun platform was developed in 2011, by the University of Chile. The platform allowed the measurement of various QoS characteristics, using hardware for fixed services and an app for mobile services. The fixed measurements ran until 2013 at which point the results were handed over to SUBTEL to inform the development of its QoS data-gathering programme. The mobile app is still available today.

The Adkintun case is an example of where an NRA has used a third party to help define the requirements of its transparency reporting. The arrangement also provided knowledge transfer to the NRA, to assist with capacity building on net-neutrality issues.

Case study 2: Sistema de Transferencia de Información (STI), Chile

The STI portal provides an automated method for ISPs to upload the QoS data they are required to report to SUBTEL under net-neutrality regulations. The portal accepts data in plain text, and SUBTEL is currently developing internal tools to analyse the large volume of data it gathers.

This is an example of a standardised data-gathering mechanism that an NRA can use to collect large amounts of data from ISPs for statistical analysis. Although SUBTEL is currently focused on gathering QoS data, it considers that the portal could be used to accept net-neutrality-specific data if this were required. This approach could be implemented by other regulators.

Case study 3: Netalyzr, USA

Netalyzr is a software tool for measuring various Internet performance metrics. Netalyzr was joint winner of the FCC's 2011 competition for innovative research and useful apps that further the understanding of Internet connectivity and network science. The metrics that the tool measures may be instructive in detecting certain traffic-affecting practices (e.g. blocking), although the FCC does not make systematic use of the tool.

The Netalyzr case is an example of an initiative involving a third-party which is only loosely affiliated to the NRA, but may still provide a useful deterrent against practices which violate net neutrality. The combination of third-party initiatives and an established complaints process may be enough to make an NRA aware of any major net-neutrality violations.

Case study 4: Measuring Broadband America programme, USA

The Measuring Broadband America programme uses a panel of volunteers to measure various QoS characteristics of fixed and mobile broadband. Fixed broadband measurements are made using hardware probes, whereas mobile broadband measurements are made via an app. By participating in the programme, ISPs can also automatically meet part of the transparency requirements required by the Open Internet Order.

Measuring Broadband America is an example of a measurement initiative set up by the NRA which ensures automatic compliance with transparency requirements for the ISPs which take part. Although the programme only covers QoS measurement, the same approach could be used for net-neutrality-specific measurements.

1.4 Lessons learnt and concluding remarks

The analysis undertaken for this study provides the following general lessons which may be of use for European NRAs and BEREC while they are implementing EU net-neutrality regulation:

- Quality of service (QoS) clearly has an impact on net neutrality, but the two concepts are quite distinct. Regulators in some markets are actively monitoring QoS, but have chosen to rely on a range of different methods to monitor net neutrality, such as qualitative reporting of traffic-management practices by the ISPs, the 'seeding' of third-party initiatives, and having an established complaint system.

- The important role of the complaint systems in the USA and Chile means that enforcement in these two countries has a primarily ex-post character (in contrast to the EU, where Regulation 2015/2120 requires NRAs to monitor proactively, on an ex-ante basis).

- In some regulatory regimes, existing mechanisms and powers for tackling anti-competitive behaviour are chosen to be relied upon for some non-net-neutral practices, which provides regulators with future discretion. In Chile, tolerance of traffic management is checked against competition principles. In the USA, the FCC relies on telecoms law that was designed prior to the Internet era, to ensure reasonableness of prices, prohibit discrimination, respond to complaints, and impose penalties

- Third-party organisations can provide useful complements to the NRAs, in terms of expertise and capacity building in measurement systems suitable for the detection of certain types of net-neutrality violations. Examples include the University of Chile and the Broadband Internet Technical Advisory Group (BITAG) in the USA.

- Regulators are considering non-net neutrality practices across both fixed and mobile networks. In the case of mobile networks, crowd-sourced smartphone app-based approaches for gathering measurements are being used in both Chile and the USA.

- Many different tools are available to detect practices which may violate net neutrality (either ex ante or ex post), but it is unlikely that any single tool can provide a comprehensive solution. Incidents such as the Comcast/BitTorrent episode in the USA[4] (see Section 3.2.3) demonstrate that regulators will have difficulty anticipating every possible form of net-neutrality abuse in advance. In the EU/EEA, NRAs are obliged to actively monitor non-net-neutral practices themselves. The technical requirements of doing so need to be carefully thought through and specified, and multiple tools or methods are likely to be required. This may imply the need, not for a *tool*, but for a *toolkit* that can grow over time as new risks are identified and as new forms of abuse are encountered.

4 Comcast had been blocking peer-to-peer network *uploads*, a form of degradation that had not been anticipated by regulatory experts. It was fortuitous that Rob Topolski, a network engineer, amateur musician and broadband subscriber happened to have a packet monitor and the competence to understand what he was seeing.

2 Introduction

2.1 Aim of the study

BEREC commissioned Analysys Mason and Scott Marcus to study the approach taken by NRAs in selected non-European benchmark countries to address net-neutrality issues. The benchmark countries are:

- Chile (SUBTEL)
- India (TRAI)
- USA (FCC).

The study aims to contribute to an informed public debate and constitute a source of practical information for European NRAs and BEREC while they are implementing EU regulation 2015/2120.[5] The study also aims to help BEREC and European NRAs to define their options for addressing net-neutrality issues and identify the requirements and challenges they may face in future. Comparisons of the European framework to the benchmark countries are not included in the study. It should be noted that the study does not include comparisons between the benchmark countries and the European regulatory framework.

The study has focused on how NRAs in the benchmark countries monitor and enforce net-neutrality principles. However, a consideration of wider net-neutrality issues is also included.

2.2 Summary of net neutrality

A useful summary of the issue of net neutrality is provided in a consultation paper that Indian NRA TRAI issued on OTT services:[6]

"Net neutrality (NN) is generally construed to mean that [ISPs] must treat all internet traffic on an equal basis, no matter its type or origin of content or means used to transmit packets. All points in a network should be able to connect to all other points in the network and service providers should be able to deliver traffic from one point to another seamlessly, without any differentiation on speed, access or price. The principle simply means that all internet traffic should be treated equally."

It should be noted that we are not using an absolute definition of net neutrality, but rather the general principle, as each country has a different version that it is looking at. Net neutrality has taken on different meanings in different countries. They are similar, but they are not the same, and they have somewhat different implications for the rules to be enforced. Many countries choose not to have a legal definition of net neutrality as such, but instead identify violations or identify a number of principles.

5 We note that this regulation is already complemented by implementation guidelines from BEREC.

6 See http://www.trai.gov.in/sites/default/files/OTT-CP-27032015.pdf

2.3 Approach to conducting the study

Analysys Mason and Scott Marcus have conducted this study using a combination of desk research and interviews with in-country stakeholders. The key documents that have informed the study are referenced in footnotes throughout this report.

By interviewing highly knowledgeable stakeholders from each of the benchmark countries we have been able to gather insights from both regulatory and industry viewpoints. We note that many of the interviewees asked to remain anonymous.

2.4 Structure of this document

The remainder of this document is laid out as follows:

- Section 3 provides a structured review of the approach taken to tackling net-neutrality issues in each benchmark country
- Section 4 presents case studies from the benchmark countries, detailing the detection/ characterisation tools and techniques used in those countries
- Section 5 summarises lessons learnt and provides conclusions relevant to BEREC member organisations.

Annex A provides a wide-ranging review of tools and techniques available to detect and characterise non-net-neutral practices.

3 Approach to tackling net neutrality in benchmark countries

In this section we provide a structured review of the approach taken to tackling net neutrality in the three benchmark countries (Chile, India and the USA). We discuss:

- the evolution of net-neutrality rules over time (Section 3.1)
- non-net-neutral practices (Section 3.2)
- transparency obligations on ISPs in relation to practices which may affect net neutrality (Section 3.3)
- monitoring and supervision by NRAs (Section 3.4)
- legal mechanisms for enforcement of net neutrality by NRAs (Section 3.5)
- reporting by NRAs (Section 3.6).

In each subsection we summarise the relevant information for each benchmark country (Chile, India and the USA).

3.1 The evolution of net-neutrality rules over time

To explain the methods and tools that the three countries employ to monitor possible deviations from the principles of net neutrality, it is necessary to first describe the rules that they are seeking to enforce.

3.1.1 Chile

Chile was the first country in the world to enshrine the principles of net neutrality into law,[7] which was enacted in 2010. The law aimed to guarantee a very general principle of no blocking or obstacles to the flow of information on the Internet. The approach is principles-based rather than rules-based: it aims to guarantee users' access to content, and provide entrepreneurs with a platform on which to innovate.[8]

The net-neutrality law in Chile has the following principles:

- **Transparency**: ISPs must publish detailed information about their retail offers, indicating the upload and download speeds, download limits, traffic-management measures, among other aspects.
- **No blocking of content and applications**: The law guarantees the right to freely access any type of legal content or service on the Internet, without the provider being able to deny such access. These include peer-to-peer (P2P) file downloads, online video, online games and IP telephony, among others. Traffic management is allowed, if the traffic-management measures are clearly specified to end users as part of the commercial offer and these measures do not harm free competition.

7 See http://www.regulatel.org/wordpress/wp-content/uploads/2015/07/4.Neutralidad_de_la_red_version%20final.pdf

8 Source: interview with industry stakeholder.

- **Quality indicators**: ISPs must carry out measurements of technical QoS indicators, based on protocols approved by SUBTEL. The results are reported to SUBTEL on a quarterly basis.

Following the law, a guideline (the "reglamento") was implemented. This included specific guidance on the minimum conditions that Internet access providers must meet, regarding the transparency obligations. In particular, they are required to post information about the service on their website (and keep it up to date), encompassing: available access speeds, level of aggregation or overselling of the link, availability of the link over time, service repair times, use of management tools or traffic management, as well as those elements specific to the type of service offered and that correspond to generally applied international quality standards. (The requirements of the reglamento are discussed in more detail in Section 3.3.1.)

There are two other points that should be noted regarding net-neutrality regulation in Chile:

- SUBTEL considers that the principles of net neutrality apply equally to fixed and mobile networks, although it has acknowledged in the regulation that there are greater difficulties in guaranteeing QoS on mobile networks than on fixed.
- In addition to the issue of users' access to content and services (which may be affected by price differentiation, QoS or blocking), SUBTEL also considers the terms and conditions under which networks agree to exchange traffic (peering and transit) at Internet exchange points (IXPs).

3.1.2 India

TRAI recently issued two decisions which are relevant to net neutrality.

The first decision, "Prohibition of discriminatory tariffs for data services",[9] provides regulation to tackle the specific *commercial* issue of zero rating. There are two key elements to the regulation:

- No ISP can offer or charge discriminatory tariffs for data services based on content
- No ISP shall enter any arrangement, agreement or contract, by whatever name, with any person, natural or legal, that has the effect of causing discriminatory tariffs for data services being offered or charged by the service provider for the purpose of evading the prohibition in this regulation.

The regulation is wide ranging. The term "content" is defined as "all content, applications, services and any other data, including its end-point information, that can be accessed or transmitted over the internet". There are, however, some exclusions from the regulation: access to emergency services is not included, nor are tariffs for services provided over "closed electronic communications networks" (unless such tariffs are being offered in order to evade the regulation). The regulation allows TRAI to order ISPs to remove discriminatory tariffs, and also pay a fine of INR50 000 (approximately EUR700) per day of contravention, up to a maximum of INR5 million (approximately EUR70 000).

9 See http://www.trai.gov.in/notifications/press-release/trai-releases-prohibition-discriminatory-tariffs-data-services

The second decision, "Encouraging Data usage in Rural Areas through provisioning of Free Data",[10] provides clarification on what ISPs can do to encourage take-up of Internet services (which was a key reason cited by proponents of zero-rated tariffs). The decision recommends that small amounts of data (e.g. 100MB per month) be made available to users in rural areas free of charge. The data should be funded by the Universal Service Obligation Fund (USOF). Crucially, it is recommended that such schemes are facilitated by an ISP-agnostic third-party "aggregator".

Regulations to consider the wider aspects of net neutrality are not yet in place. TRAI recently held a consultation on the wider aspects of net-neutrality regulation, which closed on 26 April 2017; at the time of writing no decision had been published.

3.1.3 USA

The legislative and policy history of net neutrality in the USA is long and complex, so the discussion here focuses on those aspects needed to understand current monitoring and enforcement.[11]

The immediately relevant history of net neutrality in the USA began with an Open Internet Order, adopted in December 2010.[12] That Open Internet Order included a *Transparency Rule*, requiring a provider of broadband Internet access service to publicly disclose accurate information regarding the network-management practices, performance, and commercial terms of its broadband Internet access services, sufficient for consumers to make informed choices regarding use of such services. The Open Internet Order of 2010 also imposed rules against blocking or unreasonable discrimination against *fixed* network services (i.e. it did not cover mobile[13]).

The US network operator Verizon filed a suit against the Open Internet Order of 2010, arguing that the FCC had exceeded its authority. In January 2014, the court largely sided with Verizon,[14] and overturned large parts of the Open Internet Order of 2010, including the rules against blocking or unreasonable discrimination against fixed network services; however, the court let the Transparency Rule stand.

The Open Internet Order that was enacted in 2015[15] retains (a somewhat clearer version of) the Transparency Rule from the 2010 order. It also includes three key new rules:

---

10 See http://www.trai.gov.in/notifications/press-release/trai-issues-recommendations-encouraging-data-usage-rural-areas-through

11 For additional details, see J. Scott Marcus (2014), *Network Neutrality Revisited: Challenges and Responses in the EU and in the US*, a study on behalf of the European Parliament's IMCO Committee, IP/A/IMCO/2014-02, PE 518.751, available at http://www.europarl.europa.eu/RegData/etudes/STUD/2014/518751/IPOL_STU%282014%29518751_EN.pdf viewed 6 May 2017, Section 6.1.1.

12 US FCC, Report and Order, In the Matter of Preserving the Open Internet; Broadband Industry Practices; GN Docket No. 09-191, WC Docket No. 07-52, 23 December 2010.

13 There was a separate, but much weaker, no-blocking rule for mobile.

14 United States Court of Appeals for the District of Columbia Circuit (2014), Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014).

15 Protecting and Promoting the Open Internet, GN Docket No. 14-28, Report & Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601 (2015).

- **No blocking**: ISPs shall not block lawful content, applications, services, or non-harmful devices, subject to reasonable network management[16]
- **No throttling**: ISPs shall not impair or degrade lawful Internet traffic on the basis of Internet content, application, or service, or use of a non-harmful device, subject to reasonable network management[17]
- **No paid prioritisation**: ISPs shall not engage in paid prioritisation. "'Paid prioritization' refers to the management of a broadband provider's network to directly or indirectly favour some traffic over other traffic […]".[18]

The 2015 Order also added the explicit consideration of mobile services.

Specialised services[19] are not explicitly defined in the 2015 Order. However, the 2015 Order states that "*other non-broadband Internet access service data services could be provided in a manner that undermines the purpose of the open Internet rules and that will not be permitted. The [FCC] expressly reserves the authority to take action if a service is, in fact, providing the functional equivalent of broadband Internet access service or is being used to evade the open Internet rules*."[20] Therefore, specialised services can be offered in the USA, but not in a way that would undermine the purpose of the Open Internet Order.

Following the change of US government in January 2017, the USA also has a new FCC Chairman, a new Republican Party majority among the FCC Commissioners, and Republican majorities in both houses of the US Congress. Those in charge today do not appear to share the views of their predecessors regarding net neutrality. Some changes are already visible, while others are difficult to predict. In light of this uncertainty, this study has primarily looked at US practice in the recent past, rather than speculating on how US practice may change in the immediate future.

3.2 Non-net-neutral practices

Non-net-neutral practices are any practices encountered by an NRA which are suspected of violating the national principles of net neutrality, such as zero rating (reducing the charge for certain traffic), plus rating (increasing the charge for certain traffic), prioritisation, throttling, blocking and modifying traffic. Practices which were investigated, but subsequently found not to be in violation of net neutrality, are also considered below.

16 Para. 15, Open Internet Order (2015).

17 Paras. 16–17, Open Internet Order (2015).

18 Para. 18, Open Internet Order (2015).

19 Specialised services are services which are delivered over the same infrastructure as Internet services, but do not include a connection to the Internet. Specialised services may use different quality parameters, such as prioritised traffic. Examples include IPTV, VoLTE, VPNs and emergency services.

20 Para. 35, Open Internet Order (2015). For example, IPTV must not undermine competing OTT TV services.

3.2.1 Chile

A widely-discussed net-neutrality issue experienced in Chile was the practice of zero rating for social networks. ISPs in Chile were offering access to certain social network websites for free, and only charging users when they followed links that took them outside the social network service onto the wider Internet.

Chile does not have a specific law or regulation on zero rating. However, SUBTEL issued a letter clarifying its position regarding zero rating to the relevant companies on 27 May 2014, ordering them to withdraw the promotions called "Free Social Networks". The letter highlighted the relevant section of the law, and instructed the companies to end these promotions.

SUBTEL also received some complaints about port blocking in relation to surveillance cameras, but this was resolved via a change in the modem equipment (following SUBTEL's intervention).

3.2.2 India

In India, the major non-net-neutral practices encountered to date have also involved zero rating, i.e. the practice of charging nothing for certain types of traffic. A timeline of zero-rating events in India is as follows:[21]

- In February 2015, Facebook launched *Internet.org* in India, with Reliance Communications (also referred to as "Free Basics"). It aimed to provide free access to 38 websites (including the Bing search engine), through an app[22]
- In April 2015, Airtel announced the "Airtel Zero" scheme. Under the scheme, app firms signed a contract with Airtel, and Airtel provided the traffic associated with these apps free of charge
- On 27 March 2015, TRAI released a consultation paper on OTT services and net neutrality for public feedback
- On 23 April 2015, various organisations involved in the Free Software Movement of India organised protests in several cities across India[23]
- Towards the end of 2015, TRAI temporarily banned[24] Facebook's "Free Basics" zero-rated app, for an undisclosed time
- On 9 December 2015, TRAI issued a consultation paper on 'Differential Pricing for Data Services'
- On 8 February 2016, TRAI issued the 'Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016'. These regulations prevent ISPs from charging discriminatory tariffs for data services on the basis of content (see Section 3.5 for further discussion of the discriminatory data tariff regulation)

21 See http://trai.gov.in/telecom/net-neutrality

22 Source: *The Economic Times*, 9 April 2015.

23 See http://www.cxotoday.com/story/15-key-milestones-in-net-neutrality/

24 See http://www.gadgetsnow.com/tech-news/Put-FBs-Free-Basics-service-on-hold-TRAI-tells-Reliance-Communications/articleshow/50290490.cms

- Following introduction of the Discriminatory Tariffs regulation, Airtel cancelled plans for its "Airtel Zero" scheme.[25]

In its recently closed consultation on net neutrality, TRAI has considered wider practices that may contravene net-neutrality principles.[26] Based on a review of net-neutrality regulations around the world, TRAI identifies the following practices as being non-net neutral:

- blocking
- throttling
- preferential treatment.

3.2.3 USA

The FCC does not actively monitor for deviations from network neutrality. There is a well-established process for the FCC receiving complaints from any interested party.

In the past, the FCC addressed several cases of alleged deviation from net neutrality. The best known among these are the Madison River case, and the Comcast / BitTorrent case.[27] Among the more recent cases, the Comcast / Netflix case is perhaps the most prominent.

Madison River

The FCC's enforcement action *In the Matter of Madison River Communications, LLC and affiliated companies*[28] is often cited as an example of net-neutrality policy in action. Unfortunately, little is publicly known about the case, inasmuch as it was an action of the Enforcement Bureau of the FCC and thus subject to confidentiality.

Madison River Communications provided telephone and broadband Internet services in Alabama, North Carolina, Georgia, Mississippi and Illinois. The FCC investigated "allegations that Madison River was blocking ports used for VoIP applications, thereby affecting customers' ability to use VoIP through one or more VoIP service providers." Presumably, Madison River's behaviour would have been profitable had the FCC not intervened.

To conclude the case, Madison River and the FCC entered into a "consent decree": in exchange for the FCC's dropping the matter and promising not to investigate further in the absence of new complaints, Madison River agreed that it would "not block ports used for VoIP applications or

25 See http://www.medianama.com/2017/05/223-eros-now-gaana-binge-on/

26 See http://www.trai.gov.in/telecom/net-neutrality

27 The review of these old cases is based on an earlier study, Scott Marcus (2014), *Network Neutrality Revisited: Challenges and Responses in the EU and in the US*", on behalf of the European Parliament's IMCO Committee, IP/A/IMCO/2014-02, PE 518.751; see http://www.europarl.europa.eu/RegData/etudes/STUD/2014/518751/IPOL_STU%282014%29518751_EN.pdf viewed 6 May 2017, p.38 and p.85. See also Kenneth R. Carter, J. Scott Marcus and Christian Wernick (2010), *Network Neutrality: Implications for Europe*.

28 Federal Communications Commission, *In the Matter of Madison River Communications, LLC and affiliated companies*, DA 05-543, File No. EB-05-IH-0110.

otherwise prevent customers from using VoIP applications." In addition, Madison River agreed to make a "voluntary" contribution of USD15 000 to the US Treasury.[28]

The FCC's ruling did not provide any basis for FCC jurisdiction in the matter, nor did it indicate exactly what rules, if any, had been violated. Consequently, the consent decree did not provide useful guidance or concrete rules for future reference.[29]

Comcast / BitTorrent

In November 2007, the FCC received a complaint on behalf of Rob Topolski, a network engineer, amateur musician and broadband subscriber of Comcast (the USA's largest broadband ISP). Topolski had discovered that no one was able to download his uncopyrighted music from BitTorrent. According to the complaint, Comcast was actively interfering with Topolski's use of BitTorrent by masquerading as another computer and using reset packets to stop the transmission of files in various peer-to-peer networks, notably BitTorrent. "It's like a telephone operator breaking into a conversation, telling each person in the voice of the other, 'sorry, I have to hang up, goodbye.'"[30] The reset packets did not technically block the application, but delayed it sufficiently that it was effectively blocked. Comcast customers had not been notified of the practice.[31]

A Comcast spokesman stated at the time, "Comcast does not block access to any applications, including BitTorrent."[32] While this statement might have been technically true, it was arguably misleading.

In the complaint that Free Press (a public-interest organisation) filed with the FCC,[33] it asked the FCC to declare "that an Internet service provider violates the FCC's Internet Policy Statement[34] when it intentionally degrades a targeted Internet application."[35] The Policy Statement, however, was merely a statement of intent, not an ex-ante rule.

The FCC claimed jurisdiction to enforce "federal policy",[36] without, however, first creating any ex-ante rules to enforce. In the adjudicatory proceeding that followed, the FCC sought to determine

29 Kenneth R. Carter, J. Scott Marcus and Christian Wernick (2010), *Network Neutrality: Implications for Europe*.

30 Brooke Gladstone, "Please Don't Share". On the Media, WNYC, New York Public Radio, 26 October 2007.

31 This section draws on Scott Marcus (2014), *Network Neutrality Revisited: Challenges and Responses in the EU and in the US*, a study on behalf of the European Parliament's IMCO Committee, IP/A/IMCO/2014-02, PE 518.751; see http://www.europarl.europa.eu/RegData/etudes/STUD/2014/518751/IPOL_STU%282014%29518751_EN.pdf viewed 6 May 2017, p.85. See also Kenneth R. Carter, J. Scott Marcus and Christian Wernick (2010), *Network Neutrality: Implications for Europe*.

32 Brooke Gladstone, "Please Don't Share". On the Media, WNYC, New York Public Radio, 26 October 2007.

33 Formal Complaint of Free Press and Public Knowledge against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications, File No. EB-08-IH-1518 (1 November 2007) (Free Press Complaint).

34 Federal Communications Commission, Internet Policy Statement, 20 FCC Rcd at 14988.

35 Federal Communications Commission, Memorandum Opinion and Order, In the Matters of Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications Broadband Industry Practices Petition of Free Press et al. for Declaratory Ruling that Degrading an Internet Application Violates the FCC's Internet Policy Statement and Does Not Meet an Exception for "Reasonable Network Management, WC Docket No. 07-52 (20 August 2008).

36 *Ibid*, para 15.

whether Comcast's actions were violating consumers' right to "run applications and use services of their choice," and the degree to which Comcast's action might constitute "reasonable network management practices". The FCC found the manner in which Comcast was resetting TCP connections without regard to network traffic load to be unreasonable. The FCC suggested that bandwidth caps and/or charges for excess traffic might have been reasonable. The FCC declined to consider whether Comcast's failure to disclose its practices to subscribers was in violation of FCC policy. In summary, the FCC found that Comcast had interfered with the ability of its broadband customers to access peer-to-peer applications such as BitTorrent.

Comcast agreed to end the practice; however, it challenged the legal basis on which the FCC had ordered it to do so. Comcast argued that the FCC had acted improperly, first by enforcing a 'rule' that was not in fact a rule, and circumventing the normal bureaucratic safeguards (notably, the requirements of the Administrative Procedures Act); and second, that the FCC lacked authority to issue such a rule in the first place for an information service. The court indeed found that the FCC had failed to demonstrate its authority, and therefore vacated (lifted) the FCC's order.[37]

Comcast/Netflix dispute

Of greater current relevance is the long-running 2013–2014 dispute between cable-network operator Comcast and OTT video provider Netflix (or more precisely, the network operators that carried traffic on behalf of Netflix). Comcast (the largest single retail broadband ISP in the USA) demanded, and Netflix resisted, payments for video streaming traffic carried between Netflix and consumers who viewed Netflix videos using Comcast's broadband network.

As a result of the dispute, Comcast declined to upgrade interconnection capacity[38] to Cogent, a network operator that carried traffic on behalf of Netflix.[39] The limited interconnect capacity caused a visible slowing of traffic to Netflix customers, arguably to the detriment of all concerned.[40] In February 2014, Netflix reached a commercial agreement involving payments to Comcast, thus resolving the dispute. Over the subsequent three months, performance delivered to Netflix customers on Comcast's network improved dramatically (see Figure 2).[41] Netflix CEO Reed Hastings made a public statement that: "Netflix believes strong net neutrality is critical, but in the near term we will in cases pay the toll to the powerful ISPs to protect our consumer experience. When we do so, we

37 See Comcast vs. FCC, United States Court of Appeals for the District of Columbia Circuit, argued 8 January 2010, decided 6 April 2010, No. 08-1291.

38 Comcast acts as backbone as well as an ISP.

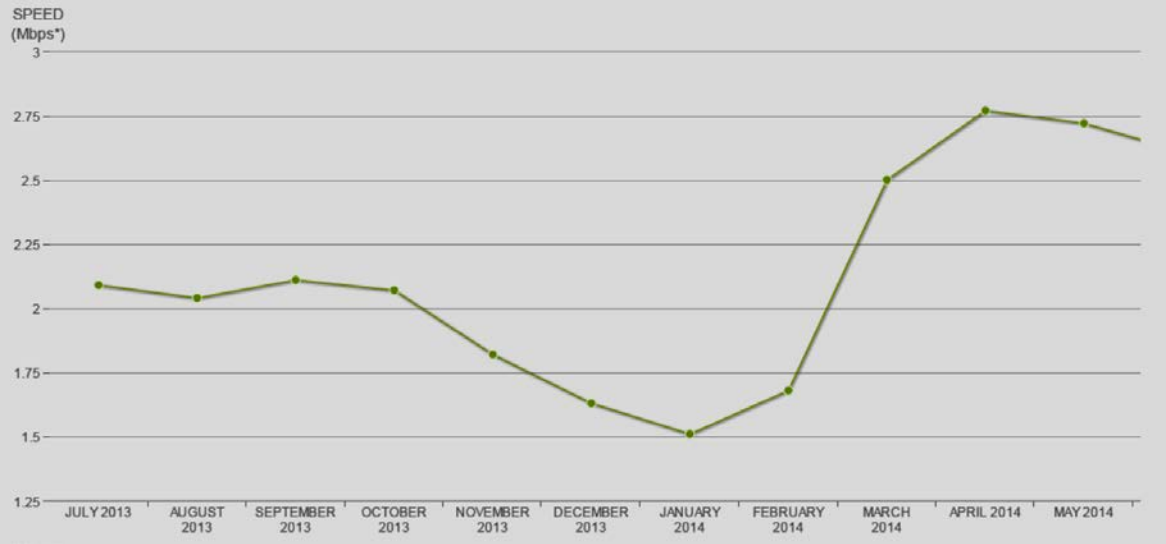
39 Netflix uses a range of means to deliver its content, including not only Amazon but also CDN solutions including Akamai, LimeLight and Level 3. See Vijay Kumar Adhikari, Yang Guo, Fang Hao, Matteo Varvello, Volker Hilt, Moritz Steiner and Zhi-Li Zhang (2012), *Unreeling Netflix: Understanding and Improving Multi-CDN Movie Delivery*.

40 See Netflix public performance statistics at http://ispspeedindex.netflix.com/results/usa/graph (viewed on 26 August 2014).

41 See J. Scott Marcus (2014), "Network Neutrality Revisited: Challenges and Responses in the EU and in the US", a study on behalf of the European Parliament's IMCO Committee, IP/A/IMCO/2014-02, PE 518.751, http://www.europarl.europa.eu/RegData/etudes/STUD/2014/518751/IPOL_STU%282014%29518751_EN.pdf (viewed 6 May 2017), pp.46–47. See also Reed Hasting (2014), 'Internet Tolls And The Case For Strong net neutrality', 20 March 2014, at http://blog.netflix.com/2014/03/internet-tolls-and-case-for-strong-net.html

don't pay for priority access against competitors, just for interconnection. A few weeks ago, we agreed to pay Comcast and our members are now getting a good experience again."[42]

Figure 2: Performance of Netflix traffic to its customers over Comcast's network (July 2013 to May 2014) [Source: Netflix USA ISP Speed Index Results Graph[43]]



It is not entirely clear whether an activist FCC would have been able to take action had the Open Internet Order of 2015 been in place at the time of the Comcast/Netflix dispute. The Order makes clear the FCC's jurisdiction over interconnection, inasmuch as interconnection is recognised as part of the Broadband Internet Access Service (BIAS) service, and hence is covered under Title II of the Communications Act of 1934 as amended, specifically including Sections 201 and 202 (which prohibit unreasonable and unreasonably discriminatory practices). The Open Internet Order of 2015 "does not [however] apply the open Internet rules to interconnection". At the same time, the 2015 Order specifically notes that "consumers have been subject to degradation resulting from commercial disagreements, perhaps most notably in a series of disputes between Netflix and large last-mile broadband providers." The 2015 Order adopts a 'watch-and-wait' approach to interconnection, but for the first time "provides authority to consider claims involving interconnection, a process that is sure to bring greater understanding to the Commission".[44] In sum, the FCC has asserted authority to act on an ex-post basis, but has not established ex-ante rules.

AT&T's 'unlimited' broadband plans

A significant FCC action involved AT&T's so-called *unlimited* broadband plans. In 2011, the FCC sought to impose a fine of USD100 million on AT&T Mobility for alleged violations of the Transparency rule of the Open Internet Order of 2010. "In 2011, AT&T implemented a 'Maximum Bit Rate' policy and capped the maximum data speeds for unlimited customers after they used a set

42 Reed Hasting (2014), "Internet Tolls And The Case For Strong Net Neutrality", 20 March 2014; see http://blog.netflix.com/2014/03/internet-tolls-and-case-for-strong-net.html

43 See http://ispspeedindex.netflix.com/results/usa/graph (viewed on 26 August 2014).

44 Paras. 38, 40 and 41, Open Internet Order 2015.

amount of data within a billing cycle. The capped speeds were much slower than the normal network speeds AT&T advertised and significantly impaired the ability of AT&T customers to access the Internet or use data applications for the remainder of the billing cycle. […] The FCC's investigation alleges that AT&T severely slowed down the data speeds for customers with unlimited data plans and that the company failed to adequately notify its customers that they could receive speeds slower than the normal network speeds AT&T advertised."[45]

As of June 2017, the fine has not been collected, and it is quite likely that it never will be.[46] This is not particularly unusual – the FCC is known for imposing large fines and then neglecting to follow through promptly on collection.[47] In this case, the change in leadership at national level and in the chairmanship of the FCC earlier in 2017 apparently means that the current FCC has no appetite to pursue the case.

At the same time, the US Federal Trade Commission (FTC), which had attempted to fine AT&T for the same throttling violations prior to the FCC's Open Internet Order of 2015 was unexpectedly blocked by a court decision in the Ninth Circuit from imposing penalties on AT&T for its conduct during the period when the FTC apparently had authority (the 2015 Order reclassified BIAS as a telecoms service, effectively blocking the FTC's authority over it). The Ninth Circuit ruled that the FTC's authority does not apply to any firm that provides telecoms service, whether the service in question is a telecoms service or not.[48] Given that the decision runs counter to several decades of consistent judicial precedent, we have some doubt as to whether it will stand; for the moment, however, it is in effect, and the FCC is endorsing and relying on it.[46]

Other issues

There have been a number of issues over the years that never rose to the level of formal FCC enforcement, such as:

- a dispute where AT&T Mobility refused to allow Apple FaceTime to operate over its cellular mobile service
- concerns over Comcast's streaming of cable content to Microsoft Xbox devices.[49]

---

45 US FCC (2015), "FCC Plans to Fine AT&T $100 Million for Misleading Consumers about Unlimited Data Plans, Violating Transparency Obligations". Note that the *Federal Trade Commission* (*FTC*) had earlier initiated a similar action against AT&T Mobility, but the adoption of the Open Internet Order of 2015 had the effect of shifting authority for consumer broadband complaints from the FTC to the FCC.

46 Wendy Davis (2017), "FCC Unlikely To Fine AT&T For Throttling Wireless Customers", MediaPost, 1 June 2017; see https://www.mediapost.com/publications/article/302168/fcc-unlikely-to-fine-att-for-throttling-wireless.html

47 Alex Byers (2015), "FCC proposes millions in fines, collects $0: The disconnect is drawing scrutiny from members of Congress", *Politico*, 23 November 2015; see http://www.politico.com/story/2015/11/fcc-fine-enforcement-scrutiny-216121

48 Steve Augustino and Jameson Dempsey (2016), "Ninth Circuit Decision in AT&T "Throttling" Case May Reset Boundaries Between FTC and FCC Jurisdiction", *CommLaw Monitor*, 30 August 2016; see http://www.commlawmonitor.com/2016/08/articles/federal-state-regulatory/ninth-circuit-decision-in-att-throttling-case-may-reset-boundaries-between-ftc-and-fcc-jurisdiction/

49 Joel Hruska (2012), "The new Comcast Xbox Xfinity app is the first nail in net neutrality's coffin", *ExtremeTech*, 28 March 2012; see https://www.extremetech.com/extreme/124041-the-new-comcast-xbox-xfinity-app-is-the-first-nail-in-net-neutralitys-coffin viewed 6 May 2017.

Concerns over the Xbox case declined as the issue turned out to have limited commercial impact.

The **Apple FaceTime case** was complex. A trade press article at the time reported that "*Apple's FaceTime, which allows live video conversations between users of Apple devices, has worked [to date] only over Wi-Fi. But Apple is changing that, opening the Skype-like service to function over cellular connections. The change comes when Apple's newest mobile-phone operating system debuts Wednesday and will spread even wider once the new iPhone 5 starts landing in hands Friday. AT&T says it will make the video-chat service available on its cellular network for those with generally more expensive, shared data plans, which the company unveiled last month. […] Among other things, the company says that it is simply a business decision to use FaceTime as a hostage to move recalcitrant customers to a new plan.*"[50]

The FCC held discussions with AT&T, an FCC advisory group published an analysis (without reaching consensus as to how to interpret the issue),[51] but no formal enforcement procedures were initiated. AT&T had been slow to respond, but eventually claimed that the practice had been an unintentional "technical glitch", that it had already resolved the issue for customers who had complained, and that it intended to resolve it for all customers.[52]

Recent developments on zero rating

A major recent initiative related to the **implementation of zero-rated plans by all US mobile network operators (MNOs)**. The Open Internet Order of 2015 did not impose a flat prohibition on zero rating, but rather committed the FCC to case-by-case analysis. The FCC noted that, in 2016, "T-Mobile significantly expanded the number of participating, zero-rated edge providers in Binge On, an offering introduced in November 2015 that zero-rated standard definition video […] Sprint has also introduced unlimited data through its Unlimited Freedom and Unlimited Freedom Premium plans, and experimented with zero-rating of the 2016 Copa America soccer tournament. AT&T and Verizon did not introduce stand-alone unlimited data plans, but have eliminated overage fees in some instances for customers who exceed their data caps and launched their own zero-rating and sponsored data programs. For example, AT&T Mobility offers a "Data Free TV" feature on its DIRECTV app that enables its broadband consumers who also subscribe to direct broadcast satellite service from AT&T's wholly-owned affiliate, DIRECTV, to view unlimited DIRECTV video content with no impact on the user's mobile data monthly allotment. […] Verizon launched its FreeBee Data and FreeBee Data 360 sponsored data programs in January 2016."[53]

This rapid expansion of zero-rated offers inspired the FCC's WTB to develop policy guidance, issued in a report late in 2016.[53] In parallel with the report, it appears that enforcement investigations

50 David Kravets (2012), "Net Neutrality Groups Challenge AT&T FaceTime Blocking", *Wired*, 18 September 2012; see https://www.wired.com/2012/09/factime-fcc-flap/ (viewed 6 May 2017). See also Open Internet Advisory Committee (OIAC) to the FCC (2013), *AT&T/FaceTime Case Study*, 20 August 2013.

51 Mobile Broadband Working Group / Open Internet Advisory Committee / Federal Communications Commission (2013), *AT&T/FaceTime Case Study*, 20 August 2013.

52 See http://www.fiercewireless.com/wireless/at-t-facetime-problems-gophone-technical-nature

53 US FCC Wireless Telecommunications Bureau (2016), "Policy Review of Mobile Broadband Operators' Sponsored Data Offerings for Zero-Rated Content and Services", pp.2–3.

were initiated against AT&T Mobility and Verizon, which were both identified in the WTB report as using zero rating in ways that might violate net-neutrality principles. The concerns raised in the WTB policy guidance were, first, that the AT&T and Verizon plans seemed to favour their own content or affiliated content over unaffiliated content (thus posing an economic risk of vertical foreclosure), and second that the market shares of AT&T and Verizon were large enough that the practice could raise competition concerns. In WTB's preliminary judgment, these factors did not appear to be present for the T-Mobile or Sprint plans. The policy guidance did not reach final conclusions, but rather noted that neither AT&T nor Verizon had yet provided an explanation that the WTB found adequate.

Among the very first actions undertaken when Ajit Pai became FCC chairman in January 2017 were (1) rescission of the WTB report on zero rating (which had no operative effect in any case), and (2) termination of any investigations of AT&T and Verizon (and T-Mobile) for their zero-rating practices.[54] Thus it is not clear how the FCC *would* have finally ruled in these cases, based on its interpretation of the Open Internet Order of 2015.

3.3 Transparency obligations on ISPs in relation to practices which may affect net neutrality

In this subsection we consider the steps taken to ensure that ISPs in benchmark countries are transparent about the services they offer, including details of traffic-management procedures.

3.3.1 Chile

The net-neutrality regulation in Chile gives specific guidance on the information which ISPs must provide to meet the requirements of the law. Of note are the following articles from the regulation:

- Article 3 requires ISPs to measure technical QoS indicators on a quarterly basis, in line with ETSI standard EG 202 057-4 V1.2.1 (2008-07)[55] (Section 5)
- Article 4 requires ISPs to measure Internet access service replacement times on a quarterly basis, in line with ETSI standard EG 202 057-1 V1.2.1 (2005-10)[56] (Section 5.5)
- Article 5 sets out the specific information that must be reported by ISPs, which includes:
  - Commercial characteristics of the Internet service, including upload/download speed, download limits and guarantees of service
  - Contention ratios
  - Technical indicators (user access time, data transmission rate, proportion of failed data transmissions, proportion of successful user accesses, delay)

54 US FCC WTB (2017), "In the Matter of Wireless Telecommunications Bureau Report: Policy Review of Mobile Broadband Operators' Sponsored Data Offerings for Zero Rated Content and Services", DA 17-127, 3 February 2017. "Today, the Bureau sent letters to AT&T Mobility, T-Mobile, and Verizon Wireless closing the inquiries into each company's sponsored data and zero-rating offerings, taking no further action. By this Order […] the Bureau now sets aside and rescinds the Policy Review Report and any and all guidance, determinations, and conclusions contained therein, including the document's draft framework."

55 See http://www.itu.int/itu-t/workprog/wp_a5_out.aspx?isn=6051

56 See http://www.etsi.org/deliver/etsi_eg/202000_202099/20205702/01.02.01_60/eg_20205702v010201p.pdf

  - Replacement time of the service
  - Quality and availability of the link
  - Traffic- and network-management practices, including their characteristics and effects on the service provided to users. The information includes the types of applications, services and protocols that are affected
- Article 6 sets out a requirement for the provision of information through SUBTEL's information-gathering portal (STI)
- Article 7 reiterates the principles of the law. In addition, it acknowledges that traffic-management practices may be carried out, providing that the actions do not affect competition. Article 7 also requires that any traffic-management actions are described to users in a clear and intelligible publication.

Of note to this study is that the information regarding traffic-management practices is submitted only in qualitative form: no numerical (measurement) data is required. Also, under the law, ISPs must submit the information via SUBTEL's STI portal (discussed in more detail in Section 4.2).

SUBTEL also monitors the commercial terms of operators' broadband plans via the information published on their websites.

There is no specific consideration of specialised services; the law applies in a general sense to all services on public (i.e. non-private) networks.

3.3.2 India

ISPs submit Performance Monitoring Reports to TRAI every quarter.[57] At present, there are no net-neutrality-specific transparency requirements placed on ISPs (although TRAI included this issue in its recent net-neutrality consultation).

The recent consultation has considered the following elements of transparency information in relation to net neutrality:

- price information and commercial terms (e.g. price, promotions, fair use and data caps)
- performance characteristics (e.g. advertised speed, actual speed, minimum speed, latency, packet loss, suitability for real-time applications)
- traffic-management practices (e.g. congestion management, bandwidth throttling, preferential treatment and blocking, and whether such practices are applied to a category/class of traffic or user, and the triggers and time periods)
- specialised services (including monitoring of their impact on delivery of Internet services).

The consultation has also looked at the following key options for how information is disclosed:

- disclosures provided directly to consumers by an ISP
- disclosures to the regulator

[57] See http://www.analytics.trai.gov.in:8001/trai/qos/method.php

- disclosures to the general public, or
- a combination of the above.

3.3.3 USA

The FCC has provided a non-exhaustive list of what information should be disclosed by ISPs. These guidelines were originally developed in 2010 (and have remained in effect, since the transparency aspects of the 2010 Open Internet Order were never overturned by the courts), but were strengthened in 2015 and expanded to include pricing aspects.

Under the Open Internet Order of 2015, ISPs are required to disclose speed, latency and packet loss. For speed, the Order talks about two distinct things: expected performance versus average performance (an average or median). ISPs that voluntarily participate in the Measuring Broadband America programme and make their results public are deemed to have complied with these requirements, and thus granted "safe harbour".

Following the release of the 2015 Order, the Chief Technologist, Office of General Counsel and Enforcement Bureau subsequently issued more detailed guidance on what should be disclosed, and how.[58] The detailed guidelines include, for instance, information on how "actual" performance compares with median or quantile speed measurements. The guidelines include both fixed and mobile broadband.

Transparency requirements relating to traffic management are similar to those in Chile, in that they are qualitative. ISPs must provide:

- details of application-specific network-management practices
- details of subscriber-triggered network-management practices
- a pointer to a web page for more details.

Regarding the requirement to describe network-management practices, ISPs are asked to "provide a brief description and a link to a full discussion that identifies application-specific [or subscriber-triggered] network management practices, when such practices are triggered, and the effect such practices could have on performance".[59]

There is no systematic, periodic review of the disclosures that ISPs make to actual or prospective customers; rather, the process is complaint-driven. The FCC may conduct spot checks to ensure that disclosures are clear.

58 US FCC (2016), "Guidance on Open Internet Transparency Rule Requirements", GN Docket No. 14-28, DA 16-569, 19 May 2016.

59 See https://apps.fcc.gov/edocs_public/attachmatch/DA-16-357A1_Rcd.pdf

3.4 Monitoring and supervision by NRAs

In this subsection we consider the steps that NRAs in the benchmark countries have taken in the past, are currently taking, or intend to take to monitor/supervise ISPs for practices that may violate net neutrality.

3.4.1 Chile

Following enactment of the net-neutrality law, SUBTEL began a programme of collaboration to help define the scope and process for ISPs to report the information required by the law. Two initiatives were enacted, both with the University of Chile:

- *"Consultancy to elaborate, implement and monitor Quality Indicators for Internet Access Service in Chile"*, which was awarded to the University's Foundation for Technologic Transfer. This resulted in the Adkintun platform, which allowed users to measure some of the quality indicators of their connections by themselves. (The Adkintun platform is described in more detail in Section 4.1, including its development into a mobile-only app.)

- *"Technical Consultancy for the review and analysis of a measuring protocol for quality indicators on Internet access"*, which was awarded to the University's Faculty of Physical Sciences and Mathematics. The output of the work was the definition of measurement methodology using probes that simulate the behaviour of users. The methodology defined the temporal and geographical requirements needed to provide a statistically representative sample.

The University of Chile's initiatives were concluded in 2013. In addition to defining the scope and process for ISP reporting, the two initiatives provided knowledge transfer to SUBTEL, to assist in building its capacity for tackling net-neutrality issues.

Another "tool" used by SUBTEL is a regular customer satisfaction survey. Every year SUBTEL carries out a survey called *Encuesta de Acceso, Usos y Usuarios de Internet*[60] (Survey of Internet access, uses and users). It takes also into account the evolution of customers' expectations, as a measure of their satisfaction with network quality.

Finally, SUBTEL is developing tools to analyse the data that comes in through the STI portal. In September 2017, SUBTEL is hoping to implement a tool that will help it to analyse the large amounts of statistical data it receives. In the first instance, the tool will be used for traffic flows, but in the longer term it could be developed to consider net-neutrality-specific issues.

3.4.2 India

At present, TRAI does not undertake any net-neutrality-specific monitoring or supervision. ISPs do throttle traffic to manage QoS, but no tools are being used to measure this.

60 See http://www.subtel.gob.cl/wp-content/uploads/2015/04/Informe-VII-Encuesta-de-Acceso-Usos-y-Usuarios-de-Internet_VF.pdf

TRAI's Analytics Portal is focused on the general QoS of India's mobile communications providers.[61] The portal allows users and service providers to explore and resolve various issues related to different telecoms services. It has three portals for different QoS parameters:

- **TRAI MySpeed Portal**: allows users to explore the mobile data experience of customers across India. Users can submit data by downloading the app and testing their data speeds
- **TRAI Drive Test Portal**: allows users to explore the results of drive tests carried out by TRAI to independently check coverage and QoS
- **TRAI QoS Analysis Portal**: allows users to explore the call drop rate of various telecoms service providers (TSPs). Through this portal the QoS performance of service providers can be identified for any specific location in India. Users can also navigate and view performance metrics from service area to district to city, and finally to the base-station (BTS) level.

There are defined complaints procedures available to consumers in India:

- a portal on TRAI's website (which receives a tracking number from the ISP involved), and
- the Consumer Redressal Forum, a quasi-judicial body which adjudicates to resolve issues.

TRAI has also considered the issue of monitoring in its recent consultation. The options being considered for monitoring of non-net-neutral practices are:

- disclosures and information from TSPs
- collection of information from users (complaints, user-experience apps, surveys, questionnaires)
- collection of information from third parties and public domain (research studies, news articles, consumer advocacy reports).

3.4.3 USA

Monitoring and supervision arrangements in the USA are primarily driven by complaints. Other than the Measuring Broadband America programme (see Section 4.4), there is no systematic or periodic monitoring.

The **Measuring Broadband America programme** serves mainly to help consumers determine whether their ISP is honouring its QoS commitment. (In the USA, there is no specific legal or regulatory obligation to deliver the advertised speed; however, a failure to do so could possibly be viewed as a misleading practice under the Transparency Rule of the Open Internet Order of 2015, or might perhaps be viewed as a violation of Sections 201 and/or 202 of the Communications Act of 1934 as amended, the general law that governs telecoms in the USA.)

At the same time, overall throttling of throughput would likely be visible in the aggregate statistics produced by the Measuring Broadband America programme, and so in that sense it can be viewed as a net-neutrality monitoring tool.

61 See http://www.analytics.trai.gov.in/

Another tool that has been recognised by the US FCC is **Netalyzr**. Netalyzr was created by the International Computer Science Institute (ICSI), an affiliate of the University of California at Berkeley. It is a Java applet that runs on the end user's device and communicates with ICSI servers in order to measure performance through the network, with a particular focus on practices of the ISP that directly serves the end user. We discuss Netalyzr in more detail in Section 4.3.

3.5 Legal mechanisms for enforcement of net neutrality by NRAs

In this subsection we provide an overview of the legal mechanisms available to NRAs in benchmark countries to enforce national net-neutrality rules on ISPs.

3.5.1 Chile

Enforcement of net neutrality in Chile is based on the 2010 law (see Section 3.1.1).

In general, SUBTEL acts mainly in response to complaints from customers. One of the most common complaints relates to degradation of service. This does not make use of net-neutrality law (which specifies no minimum level of service), and can be addressed under general telecoms law (by refunding users).

If a net-neutrality violation does occur, a fine cannot be imposed immediately. Once SUBTEL learns of the incident, it launches a "charge procedure". It then visits the ISP and inspects the infrastructure. A technical report is sent to the legal team, which prepares a statement of fine. The operator can respond to this, but then the state responds in turn with a final assessment of the matter. This is standard procedure under telecoms law, and is not specific to net neutrality.

3.5.2 India

TRAI cannot enforce net neutrality without a related regulation, and therefore it currently can only take action in situations relating to differential tariffs such as alleged zero rating (see Section 3.1.2). The current consultation on wider net-neutrality issues may result in a wider-ranging regulation under which TRAI can act on a broader range of issues.

In the event of a violation of any of its regulations (once they are defined), TRAI is able to impose monetary penalties. In particularly serious cases, the ISP's licence could be removed by the Department of Telecommunications.

3.5.3 USA

The FCC Enforcement Bureau takes responsibility for investigating complaints that are serious enough to potentially warrant fines or penalties. These investigations remain confidential until and unless a determination of apparent liability is made, at which point they become public.

The procedures followed in the case of apparent net-neutrality infractions are the same as those for any other potential violation of FCC rules.

A number of specific enforcement actions have been attempted or taken, most notably the USD100 million fine imposed on AT&T Mobility for throttling the traffic of customers who had subscribed to "unlimited" plans (see Section 3.2.3).

3.6 Reporting by NRAs

In this final subsection we explain the regime under which NRAs in benchmark countries report/publish on net-neutrality monitoring, including the items that are reported and the frequency of reporting.

3.6.1 Chile

There are no specific reports on net neutrality.

ISPs provide QoS and traffic-management-related information on a quarterly basis. Every six months, SUBTEL prepares a report on the state of the telecoms market. This is a general state-of-the-market report which includes some QoS data, but no specific reporting on net neutrality.

3.6.2 India

There is currently no net-neutral-specific reporting from TRAI. QoS information is available via the Analytics Portal, but no specific report is issued.

3.6.3 USA

The only regularly published report that relates to network neutrality is the annual report from the (fixed network) Fixed Measuring Broadband America programme. The report helps consumers to determine whether they are receiving the QoS they were promised. 13 ISPs participate in the voluntary data collection; our interviewees estimated that this covers roughly 90% of all fixed broadband subscribers in the USA.

The Measuring Broadband America programme report is discussed in more detail in Section 4.4.

There are annual reports that summarise competitive conditions for the fixed, wired network and for mobile networks (produced by WCB and the WTB, respectively). These reports contain some information that might have possible relevance to net neutrality, but they are not specifically designed to address net-neutrality issues.

4 Case studies

This section contains a set of case studies providing more detail on processes or tools for monitoring and enforcing net neutrality in the benchmark countries. The case studies are:

- Chile: Adkintun (including Adkintun Mobile)
- Chile: Sistema de Transferencia de Información (STI)
- USA: Netalyzr
- USA: Measuring Broadband America programme.

4.1 Chile: Adkintun

SUBTEL commissioned the University of Chile to develop a QoS monitoring platform for fixed and mobile Internet connections in 2011. The programme was designed to automatically and passively measure traffic passing between a user device and the network, to create a detailed picture of network characteristics.[62] A pilot programme monitoring fixed Internet connections was launched in Santiago to evaluate the effectiveness of the system, with plans to place around 1000 devices around the country following the pilot.[63] A mobile app was also developed, to monitor and evaluate the QoS delivered by mobile ISPs.

Both the fixed and mobile monitoring platforms passively monitored traffic passing between the Internet and user devices, without generating any new traffic. The resulting data sets were then sent to the university for analysis. Participation was voluntary for both the fixed and mobile monitoring platforms.

The fixed platform monitored traffic using either a modified router placed on the customer premises to check connection speeds,[63] or an application installed directly on a computer.[64] The fixed monitoring project was closed in 2013, once the objectives of the project had been achieved (see below).

The mobile platform monitors traffic via an app installed on a user's phone. The user receives daily reports on traffic consumption from a dashboard in the app, and the data is transmitted to the NIC Chile Research Labs when the phone is connected to a Wi-Fi network. The app is designed for phones running the Android operating system, and as of May 2017 it had been downloaded between 1000 and 5000 times.[65]

62 See https://issuu.com/niclabs17/docs/memoria_niclabs_2016

63 See https://www.fayerwayer.com/2012/04/chile-adkintun-el-proyecto-para-medir-la-calidad-de-la-banda-ancha-en-el-pais/

64 See http://download.cnet.com/Adkintun-Client/3000-2085_4-75765749.html

65 See https://play.google.com/store/apps/details?id=cl.niclabs.adkintunmobile

The Adkintun project was developed to help define the scope and process for ISPs to report the information required by the net-neutrality law. In addition to defining the scope and process for ISP reporting, the two initiatives provided knowledge transfer to SUBTEL, to help it build capacity for tackling net-neutrality issues.

4.2 Chile: Sistema de Transferencia de Información (STI)

SUBTEL provides the STI, a secure online portal for ISPs to submit QoS information to the regulator.[66] ISPs are required to provide information on commercial and technical aspects of their services, along with QoS data (see Figure 3 below). Data must be provided either monthly or quarterly, in plain text format.[67]

SUBTEL requires data submitted via the STI to be collected according to a protocol established as part of the net-neutrality regulation. We assume that these requirements follow the ITU's recommendations regarding the collection of quarterly QoS information for reporting.

Reported statistics are split by technology (and by segment, for fixed connections). Local traffic is defined as traffic within the ISP's network, national traffic remains within Chile, while international traffic is transmitted via submarine cables or other international transit agreements. Local and national traffic is expected to be faster than international traffic.[68,69]

Figure 3: Summary of QoS statistics reported by operators [Source: Operator websites, 2017]

	Fixed	Mobile
Technology split	Copper / fibre-optic	3G / 4G
Segment split	Local / national / international	n/a
Statistics reported	• Upload/download speed • Average speed (and deviation) • Speed in 5th and 95th percentiles • Rate of failed transmission • Average delay (and deviation)	

The data provided to SUBTEL via the STI portal contributes to SUBTEL's twice-yearly reporting on the state of Chile's telecoms market. SUBTEL uses a tool called QlikView for data visualisation. It is developing further tools to analyse the large volumes of data, and hopes to launch these in September.[67] Although the portal is currently only used for QoS-related data, SUBTEL believes it could be developed to consider net-neutrality-specific data.

66 See http://sti.subtel.cl:8080/sti/jsp/login.jsp

67 Source: interview with SUBTEL.

68 See http://www.movistar.cl/web/movistar/neutralidad-en-la-red

69 See http://personas.entel.cl/PortalPersonas/appmanager/entelpcs/personas?_nfpb=true&_pageLabel=P2760099104132 4329037346

4.3 USA: Netalyzr

Netalyzr was created by the ICSI, with funding from the US National Science Foundation (NSF), the Department of Homeland Security (DHS) Science and Technology Directorate's Cyber Security Division, and donations from Amazon, Comcast, Google and Heise Netze.

Netalyzr was joint winner of a 2011 FCC competition for innovative research and useful apps that further the understanding of Internet connectivity and network science.

It is a Java applet that runs on the end user's device and communicates with ICSI servers to measure performance through the network. Netalyzr runs a series of tests that collectively take a few minutes. The tests verify a wide range of properties of the end-user machine and the network to which it is connected, including:

- upload and download bandwidth
- network latency
- TCP connection setup latency
- size of the TCP uplink and downlink buffer
- ability to directly access a wide range of TCP port numbers
- presence or absence of a hidden proxy server
- various HTTP (i.e. the language of the web) characteristics
- various Domain Name System (DNS) characteristics, including whether each DNS resolver is responding to all types of requests
- whether there is IPv6 connectivity (the newer version of the IP), and whether the browser and the DNS support IPv6.

These tests can be illuminating, and can identify certain kinds of traffic degradation. It may be possible to identify some deviations from net neutrality using Netalyzr; however, there are other deviations that it is unlikely to uncover.[70]

Although Netalyzr was joint winner of an FCC competition, the FCC makes no systematic use of this tool. The results could, however, form the basis for a complaint to the FCC.

4.4 USA: Measuring Broadband America programme

Measuring Broadband America is the most notable active net-neutrality monitoring programme underway in the USA. The programme primarily reports on the speed, latency and packet loss that an end user receives through the participating ISP's network.

[70] Consider, for example, the TCP RESET packets that were interjected by Comcast in the BitTorrent incident. These were detected only because an end user was curious, had an Ethernet packet trace capability available, and knew enough to be able to interpret the results. It is difficult to see how a general tool like Netalyzr could identify such subtle blockages.

As the FCC explains,[71] the "*[…] measurements that provide the underlying data in [the Measuring Broadband America] Report rely both on measurement clients and measurement servers. The measurement clients reside in the homes of 4,281 panellists who receive service by the 13 participating ISPs. The participating ISPs collectively account for over 80% of U.S. residential broadband Internet connections. The panellists closely match the overall state and region statistics of Internet access connections in the United States [based on the reporting data that network operators provide to the FCC]. […] Our methodology focuses on the performance of each participating ISP's network. The metrics discussed in this Report are derived from traffic flowing between a measurement client (located within the modem or router within a panellist's home) and a measurement server. For each panellist, the tests use the measurement server for which the latency between the measurement client and server is the lowest value. As a result, the metrics measure performance along a specific path within each ISP's network, through a point of interconnection between the ISP's network and the network on which the chosen measurement server resides.*"

The statistics captured are:

- **Download speed**: measured for each client at 5-second intervals within a 30-second time interval, every 2 hours
- **Upload speed**: measured for each client at 5-second intervals within a 30-second time interval, every 2 hours
- **Latency and packet loss**: the round-trip times for approximately 2000 packets per hour, sent at randomly distributed times
- **Web browsing**: the total time to request and receive web pages from nine popular websites (including the text and images), measured every hour.[72]

Since 2011, the FCC has published annual reports on the Measuring Broadband America programme, including information on each of the indicators that has been measured.

The FCC's summarisation across the ISPs changed in 2016 in comparison with previous years, with a shift to the use of medians, quantiles and weighted averages, rather than simple averages.[73]

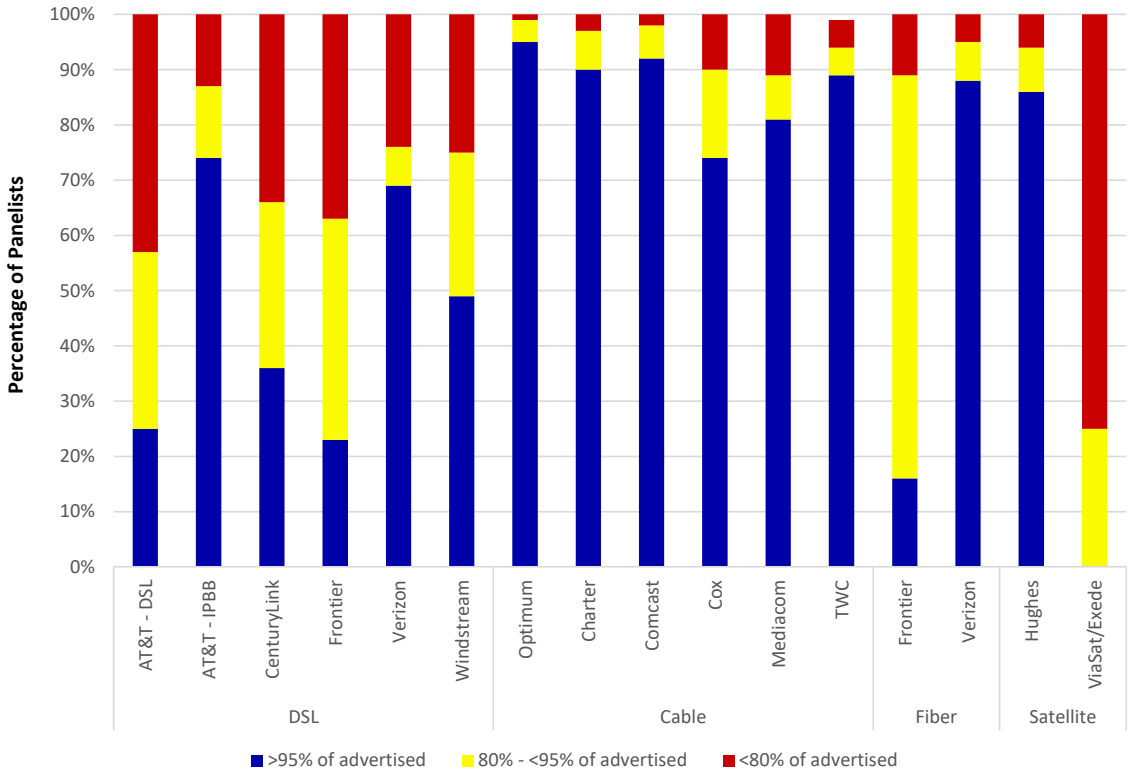
In terms of measured download speed, the annual reports provide data for each of the 13 monitored ISPs, across a number of speed brackets. In each case, data is presented on the fraction of users who receive more than 95% of the advertised speed, those who receive between 80% and 95% of the advertised speed, and those who receive less than 80% of the advertised speed (see Figure 4).

71 US FCC (2017), *2016 Measuring Broadband America: Fixed Broadband Report: A Report on Consumer Fixed Broadband Performance in the United States*, p.25.

72 *Ibid*, p.27, which provides additional detail.

73 *Ibid*, Appendix A.

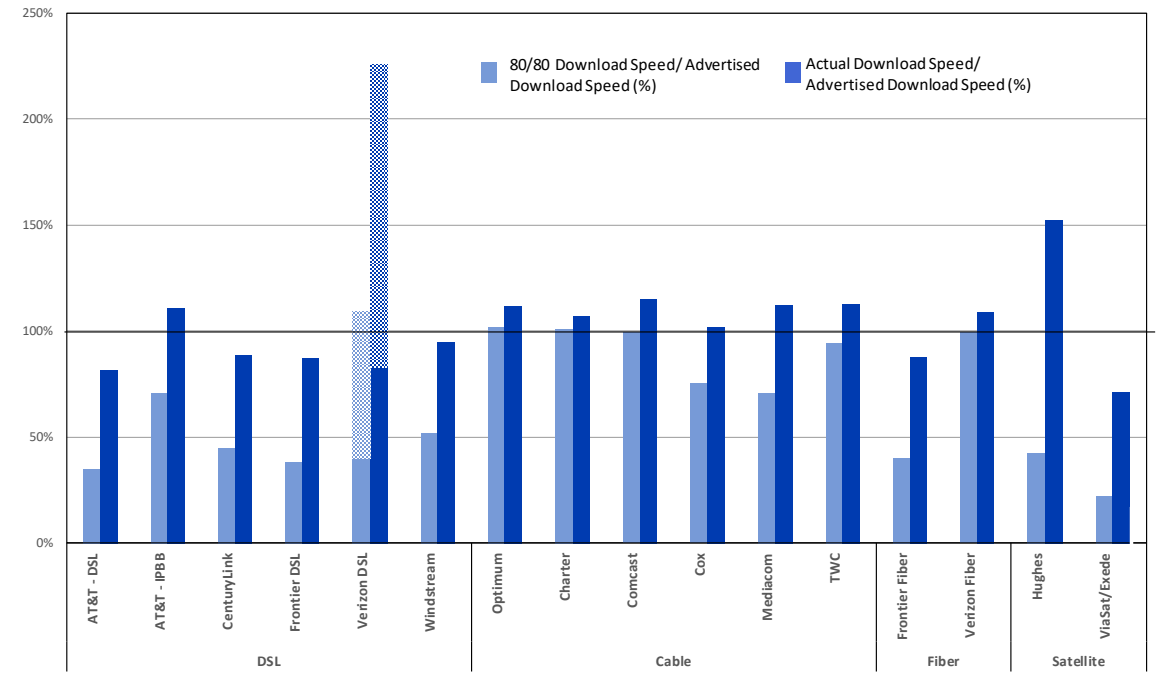
Figure 4: ISP comparison – Total – weekday peak hours, 2016 [Source: Measuring Broadband America programme online data, 2016[74]]



The annual reports also provide an '80/80' assessment; that is, the fraction of users of each of the monitored ISPs who receive more than 80% of the advertised speed during at least 80% of the peak period (see Figure 5).

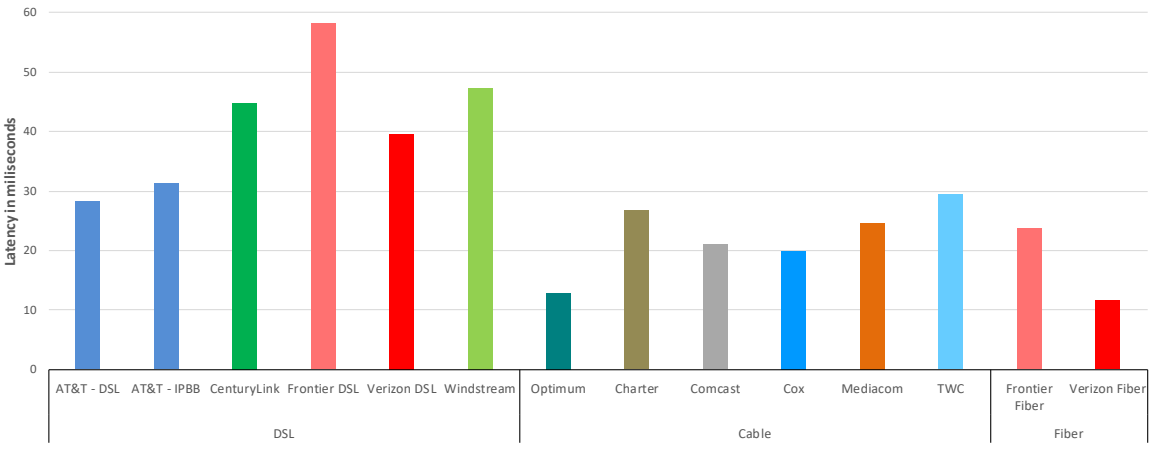
74 US FCC (2016), online data at https://www.fcc.gov/reports-research/reports/measuring-broadband-america/charts-measuring-broadband-america-2016#chart5 (viewed 10 May 2017). This corresponds to Chart 5 in the report.

Figure 5: The ratio of '80/80' consistent median download speed to advertised download speed [Source: Measuring Broadband America programme online data, 2016[75]]



The FCC's reports provide additional analysis of parameters such as packet loss and latency (see Figure 6). The latency data distinguish between terrestrial ISPs and satellite ISPs, since the round-trip time to a geosynchronous satellite is hundreds of milliseconds (due to the propagation delay for light in a vacuum).

Figure 6: Latency by ISP (terrestrial ISPs), 2016 [Source: Measuring Broadband America programme online data, 2016[75]]



75 US FCC (2016), online data available at http://data.fcc.gov/download/measuring-broadband-america/2016/chart6-fixed-2016.xlsx (viewed 10 May 2017). This corresponds to Chart 6 in the report.

Under the Open Internet Order of 2015, ISPs are required to disclose speed, latency and packet loss. In relation to speed, the Order refers to two distinct measures: "both *expected* and *actual* download and upload speeds, latency, and packet loss for each service".[76] Network operators that voluntarily participate in the Measuring Broadband America programme and make their results public are deemed to have complied with these reporting requirements, and thus granted "safe harbour".

76 Paras. 165–166. See FCC (2016), *Guidance on Open Internet Transparency Rule Requirements*, which goes on to note that the Measuring Broadband America programme "measures speed by the throughput over a five second time window, latency by the round trip time between an end user and an off-net measurement server, and packet loss by the percentage of packets transmitted from an end user to a measurement server for which no acknowledgement was received." This FCC document provides moderately detailed guidance on what should be reported.

5 Lessons learnt and concluding remarks

The analysis undertaken for this study provides the following general lessons which may be of use for European NRAs and BEREC while they are implementing EU net-neutrality regulation:

- Quality of service (QoS) clearly has an impact on net neutrality, but the two concepts are quite distinct. Regulators in some markets are actively monitoring QoS, but have chosen to rely on a range of different methods to monitor net neutrality, such as qualitative reporting of traffic-management practices by the ISPs, the 'seeding' of third-party initiatives, and having an established complaint system.

- The important role of the complaint systems in the USA and Chile means that enforcement in these two countries has a primarily ex-post character (in contrast to the EU, where Regulation 2015/2120 requires NRAs to monitor proactively, on an ex-ante basis).

- In some regulatory regimes, existing mechanisms and powers for tackling anti-competitive behaviour are chosen to be relied upon for some non-net-neutral practices, which provides regulators with future discretion. In Chile, tolerance of traffic management is checked against competition principles. In the USA, the FCC relies on telecoms law that was designed prior to the Internet era, to ensure reasonableness of prices, prohibit discrimination, respond to complaints, and impose penalties

- Third-party organisations can provide useful complements to the NRAs, in terms of expertise and capacity building in measurement systems suitable for the detection of certain types of net-neutrality violations. Examples include the University of Chile and the Broadband Internet Technical Advisory Group (BITAG) in the USA.

- Regulators are considering non-net neutrality practices across both fixed and mobile networks. In the case of mobile networks, crowd-sourced smartphone app-based approaches for gathering measurements are being used in both Chile and the USA.

- Many different tools are available to detect practices which may violate net neutrality (either ex ante or ex post), but it is unlikely that any single tool can provide a comprehensive solution. Incidents such as the Comcast/BitTorrent episode in the USA[77] (see Section 3.2.3) demonstrate that regulators will have difficulty anticipating every possible form of net-neutrality abuse in advance. In the EU/EEA, NRAs are obliged to actively monitor non-net-neutral practices themselves. The technical requirements of doing so need to be carefully thought through and specified, and multiple tools or methods are likely to be required. This may imply the need, not for a *tool*, but for a *toolkit* that can grow over time as new risks are identified and as new forms of abuse are encountered.

[77] Comcast had been blocking peer-to-peer network *uploads*, a form of degradation that had not been anticipated by regulatory experts. It was fortuitous that Rob Topolski, a network engineer, amateur musician and broadband subscriber happened to have a packet monitor and the competence to understand what he was seeing.

Annex A Tools and techniques available to detect and characterise non-net-neutral practices

In this annex we provide a wide-ranging review of tools and techniques available to detect and characterise non-net-neutral practices.

A wide range of tools and techniques were of interest to the study, including tools and techniques:

1. deployed or under deployment by NRAs
2. imposed or suggested by legal or regulatory frameworks, but not yet deployed or under deployment
3. made publicly available by third parties but currently not imposed, suggested, deployed or under deployment
4. that could be thought of (concepts), but are not currently made publicly available by third parties nor imposed, suggested, deployed or under deployment.

Because many measurement tools and concepts are publicly available on the global Internet, categories 3 and 4 above required consideration of *any* publicly available measurement tools relevant to practices and mechanisms which may violate net neutrality (not just those considered in the benchmark countries).

In Figure 7 overleaf we provide a list of publicly available measurement tools (and concepts), including a high-level summary of each.

Figure 7: List of tools and techniques for detecting and characterising non-net-neutral practices [Source: Analysys Mason, 2017]

Name	Category	Description	Purpose and capabilities
Netalyzr	Software tool	Netalyzr is a Java applet that runs on the end user's device and communicates with ICSI servers to measure performance through the network.	Netalyzr runs a series of tests that collectively take a few minutes. The tests verify a wide range of properties of the end-user machine and the network to which it is connected. See Section 4.3.
NDT[78]	Software tool	NDT (Network Diagnostic Tool) provides network configuration and performance testing to Internet users. The system uses the communication between the client program and a server to perform diagnostic functions, through a set of tests, about the poor performance of the network. As well as reporting upload and download speeds, NDT also tries to understand the problems that caused limited speeds.	NDT is designed to identify a set of performance problems, by analysing the specific conditions associated with them (such as duplex mismatch conditions on Ethernet links or incorrectly set TCP buffers in the user's computer).
Glasnost[79]	Software tool	Glasnost is a measurement tool that attempts to detect whether users are subject to traffic differentiation. Its main objective is to make ISPs' traffic-shaping policies transparent to their users. It can be used to test whether an ISP is throttling or blocking email, SSH, Flash Video, HTTP or P2P applications such as eMule.	Glasnost can detect traffic shaping in both upstream and downstream directions separately. Glasnost's tests focus on identifying whether an application is being throttled or blocked. Tests can also identify whether application flows are shaped in terms of their port numbers or their packets' payload.
ShaperProbe[80]	Software tool	ShaperProbe allows users to detect whether their ISP is applying a token-bucket shaping method to their traffic, and measure the extent of shaping. (A token bucket allows a certain number of bytes to be provided at the peak capacity of the link, whilst any remaining traffic is serviced at a lower rate.) ShaperProbe begins by measuring the link's capacity, and then it tries to detect if traffic is being shaped on the link in both upstream and downstream directions.	ShaperProbe aims to identify whether ISPs are classifying certain kinds of traffic as "low priority", and offering a different QoS for those flows of traffic. ShaperProbe can detect the shaping rate and the maximum burst before shaping begins.

78 See http://software.internet2.edu/ndt/

79 See http://broadband.mpi-sws.org/transparency/bttest-mlab.php

80 See http://netinfer.net/diffprobe/shaperprobe.html

Name	Category	Description	Purpose and capabilities
Neubot[81]	Software tool	Neubot (the network neutrality bot) is free software for gathering useful information to study net neutrality. Neubot performs periodic network-performance measurements. Three types of types of test are currently implemented: • HTTP and BitTorrent performance • raw TCP performance • MPEG DASH streaming emulation. The tests measure the application-level throughput and round-trip time (RTT) in both downlink and uplink directions. The architecture is configurable, so the user can select what tests should be carried out, at what time and for how long.	Although Neubot does not detect net-neutrality violations by itself, all information gathered is released into the public domain and is available to be analysed by any person, allowing the investigation of net-neutrality issues.
NANO[82]	Software tool	NANO (Network Access Neutrality Observatory) uses a combination of agents installed at participating clients across the Internet and statistical analysis to identify whether an ISP is discriminating against a specific service or group of clients. NANO aggregates passive measurements from multiple end users and stratifies the measurements to evaluate the impact of multiple factors.	NANO's installed agents examine the number of packets per second sent for each active flow, as well as looking for unexpected problems such as packet loss or TCP reset packets. They also monitor the load on the client computer. The main objective of NANO is to identify relationships between performance degradations and an ISP's policy.
RIPE Atlas[83]	Hardware based tool	RIPE Atlas is a global, open, distributed Internet measurement network that provides a real-time perception of the state of the Internet. RIPE Atlas collects and releases into the public domain connectivity and reachability data from thousands of devices all over the world. The hardware devices collect data on the Internet access of voluntary users. These devices are USB-powered and connected to the host's router, allowing them to perform active measurements including ping, traceroute, DNS, SSL/TLS and NTP.	RIPE Atlas continuously monitors the reachability of a network or host, via the thousands of HW devices deployed around the world. It allows the investigation and troubleshooting of reported network problems, by conducting ad-hoc connectivity checks.

81 See http://www.neubot.org/

82 See https://noise-lab.net/projects/old-projects/nano/

83 See https://atlas.ripe.net/

Name	Category	Description	Purpose and capabilities
M-Lab[84]	Hardware platform	M-Lab is a consortium of research, industry and public-interest partners dedicated to:[85] • *"Providing an open, verifiable measurement platform for global network performance"* • *"Hosting the largest open Internet performance dataset on the planet"* • *"Creating visualizations and tools to help people make sense of Internet performance"*. Some of the tools available on the M-Lab platform are NDT, Neubot, MobilePerf and Glasnost.	M-Lab is not a measurement tool, but rather it provides the infrastructure to set up a measurement platform on which measurement tools can be deployed. All the data collected by those tools is released into the public domain.
NetPolice[86]	Software tool	NetPolice enables the detection of content- and routeing-based differentiations in backbone ISPs. This tool is mainly used by large users, such as access providers or content providers, rather than by end users.	NetPolice detects traffic management that induces packet loss. It performs loss-rate measurements to detect traffic differentiation.
NPAD[87]	Software tool	NPAD (Network Path & Application Diagnostics) is a tool to diagnose end users' network-performance issues affecting their device or the network between the end user and the nearest NPAD server.	NPAD runs simple TCP tests, including throughput, RTT or packet-loss metrics. For each diagnosed problem, the server prescribes corrective actions with instructions that are easy for non-experts to understand.
BISmark[88]	Software tool	BISmark (Broadband Internet Service Benchmark) is an open platform which aims to measure the QoS performance delivered to ISPs' end users, visualising and monitoring traffic patterns through the devices inside their home network. The BISmark application is available for: • Android phones • Raspberry PI • OpenWrt routers.	BISmark software performs several active measurements such as latency, packet loss, jitter, and downlink and uplink throughput. It provides a dashboard showing performance over time and comparing performance across ISPs and regions. All data collected by BISmark is released into the public domain.

84 See https://www.measurementlab.net/
85 See https://www.measurementlab.net/about/
86 See https://web.eecs.umich.edu/~zmao/Papers/netpolice.pdf
87 See http://www.ucar.edu/npad/
88 See http://www.projectbismark.net/

Name	Category	Description	Purpose and capabilities
MobiPerf[89]	Software tool	MobiPerf is software for measuring network performance on Android mobile smartphones and tablets. The application allows the user to view the measurement results.	MobiPerf measures network properties, such as HTTP downloading latency and bandwidth, traceroute with latency to different hops, ping latency, DNS lookup latency, TCP uplink and downlink throughput, and IPv4/IPv6 compatibility. Data collected by MobiPerf is released into the public domain.
OONI[90,91]	Software tool	OONI (Open Observatory of Network Interference) is a free tool whose objective is to detect "internet censorship, traffic manipulation and signs of surveillance" all over the Internet, by gathering and processing network measurements.	The tests carried out by OONI fall into two categories: • Traffic manipulation (e.g. two-way traceroute and header filed manipulation tests) • Content blocking (e.g. RST packet detection, keyword filtering or multi-protocol traceroute). These tests allow OONI to detect blocking of websites or instant messaging apps and censorship technologies, among others. Data collected by OONI is released into the public domain.
Adkintun[92]	Hardware tool	Adkintun was a system designed by the University of Chile, NIC Chile Research Labs and SUBTEL, aimed at measuring broadband quality across the country. The system used probes (modified routers) all over the country to measure the Internet connection.	This system was intended to measure the throughput at local, national and international level by aggregating data obtained from thousands of probes. See Section 4.1.

89 See https://sites.google.com/site/mobiperfdev/

90 See https://ooni.torproject.org/about/

91 See https://www.usenix.org/system/files/conference/foci12/foci12-final12.pdf

92 See http://www.regulatel.org/wordpress/wp-content/uploads/2015/07/4.Neutralidad_de_la_red_version%20final.pdf

Name	Category	Description	Purpose and capabilities
Adkintun Mobile[93]	Software tool	Adkintun Mobile is a software tool developed by NIC Chile Research Labs that allows users to evaluate the QoS delivered by mobile ISPs and run periodic measurements. Adkintun Mobile supports Android smartphones.	Adkintun's main objective is to detect deficiencies in the service delivered by mobile ISPs. Adkintun Mobile analyses the amount of data sent and received during the day, the quality of the signal and the type of connection (e.g. 2G, 3G or 4G), among other useful data.
Dasu[94]	Software tool	Dasu is a measurement platform with an aim to monitor and measure the service provided by ISPs. It seeks to detect the variations in the performance of ISPs' networks, caused by over-booking, traffic shaping or the management of heavy users.	Dasu combines passive monitoring with active measurements of networks' P2P performance, and checks for changes in QoS that might indicate problems with the network.
NorNet[95]	Hardware tool	NorNet is a system built in Norway for measuring and experimenting with Norway's mobile broadband networks. It can test the performance of different services, including audio and video streaming applications.	NorNet's platform can be used to study variations between different paths in terms of metrics such as bandwidth, packet loss rate, congestion, delay or jitter.
SamKnows[96]	Hardware and software platform	SamKnows is a global platform whose aim is to provide fixed and mobile network-performance data to consumers, governments and ISPs. SamKnows uses both hardware- and software-based (i.e. using an application) solutions to measure Internet performance.	Depending on the solution (hardware or software-based) and the service to be measured (e.g. on-demand video streaming, multicast IPTV, web browsing, VoIP, etc.) SamKnows carries out different tests such as: • jitter of video frames • packet loss • User Datagram Protocol (UDP) download/upload speed • Internet Control Message Protocol (ICMP) round-trip latency and packet loss • page-load failure rate.

93 See http://adkintunmobile.cl/

94 See http://www.aqualab.cs.northwestern.edu/projects/115-dasu-isp-characterization-from-the-network-edge

95 See https://www.nntb.no/nornet-edge/

96 See https://www.samknows.com/

Name	Category	Description	Purpose and capabilities
CAIDA Archipelago[97]	Hardware platform	Archipelago (Ark) is a globally distributed measurement network deployed and maintained by CAIDA (Center for Applied Internet Data Analysis). It comprises 181 (second-generation Raspberry Pi) probes distributed across 60 countries. Apart from scheduled measurements, Archipelago provides access and tools to enable users to make ad-hoc measurements.	Archipelago's main objectives are to: • "reduce the effort needed to develop and deploy sophisticated large-scale measurements • provide a step toward a community-oriented measurement infrastructure by allowing collaborators to run their vetted measurement tasks on a security-hardened distributed platform". Some of the measurements regularly carried out by Archipelago focus on the detection of congestion caused by the traffic-management practices of content delivery networks (CDNs) and ISPs. Relevant tests performed are time-sequence ping and border mapping.
Tracebox[98]	Software tool	Tracebox allows the detection of middleboxes: computer networking devices that manipulate traffic flows.	Tracebox uses ICMP replies to identify modifications in the packets. It works in a similar way to the traceroute command.
TsTat[99]	Software tool	TsTat (TCP STatistic and Analysis Tool) is a passive sniffer that provides information about traffic patterns at both network and transport levels.	TsTat allows the study of novel statistics, such as the congestion window size, out-of-sequence segments or duplicated segments.

97 See http://www.caida.org/projects/ark/
98 See http://www.tracebox.org/
99 See http://tstat.polito.it/

Name	Category	Description	Purpose and capabilities
Scamper[100]	Software tool	Scamper actively analyses network topology and performance. Its tests range from simple to complex. Scamper is available for several systems, such as FreeBSD, OpenBSD, NetBSD, Linux, Mac OS X, Solaris, Windows and DragonFly.	Scamper supports IPv4 and IPv6, as well as techniques such as: • ping and traceroute • Paris and MDA traceroute • radargun • ally • mercator • sting • speedtrap • parts of tbit.
TEACUP[101]	Software platform	TEACUP (TCP Experiment Automation Controlled Using Python) enables the automation of various TCP algorithms over different emulated network path conditions, bottleneck rate limits and bottleneck queuing disciplines.	TEACUP enables the configuration of tests and experiments over the TCP protocol, and collects the data after their execution. TEACUP also provides simple tools for analysing the results.

100 See http://www.caida.org/tools/measurement/scamper/

101 See http://caia.swin.edu.au/tools/teacup/

Name	Category	Description	Purpose and capabilities
MONROE[102]	Concept	The MONROE (Measuring Mobile Broadband Networks in Europe) project is being financed by the European Union's Horizon 2020 research and innovation programme. It aims to build a dedicated infrastructure for measuring performance and Quality of Experience in both mobile broadband and Wi-Fi networks. Mobile devices will be installed on top of trains, buses and trucks, and will be capable of connecting to different service providers. These nodes devices will run different measurements and experiments, including demanding applications such as adaptive video streaming.	The main objectives of MONROE are: • "To build an open and large-scale measurement and experimental platform" distributed over multiple-countries, with multi-homing capabilities • "To use the platform for the identification of key [mobile broadband] performance parameters, thus enabling accurate, realistic and meaningful monitoring and performance assessment of such networks" • "To provide Experiments as a Service (EaaS), thus lowering the barrier for using the platform to external users, by providing well-documented tools and high-level scripts to execute experiments, collect results, and analyze data". Key performance metrics that are likely to be monitored are: • network tomography, such as performance and reliability parameters • route analytics, such as network topology inference • traffic analysis, such as passive measurements with TsTat.

102 See https://www.monroe-project.eu/

Name	Category	Description	Purpose and capabilities
Mobile Replay[103]	Concept	Mobile Replay is a proposed method for detecting traffic differentiation in mobile networks. Mobile Replay uses two main components for traffic detection: • First, it tests for differentiation by replaying real traffic traces created via users' interaction with apps • Then it conducts controlled experiments, replaying traffic over tunnelled and untunnelled connections several times. In this way, Mobile Replay can identify cases where there are meaningful differences between tunnelled and untunnelled flows, signifying differentiation.	Mobile Replay will be able to detect traffic differentiation based on attributes such as hostname, IP addresses, ports, total number of connections, payload signatures, total bandwidth and time of day, except for server-based differentiation.
DiffProbe[104]	Concept	DiffProbe (Differential Probing) is a proposed active probing method to detect whether an access ISP is performing forwarding mechanisms such as priority scheduling, variations of weighed fair queueing (WFQ), or weighted random early detection (WRED) to differentiate between some of its users' flows.	DiffProbe will aim to detect delay and loss discrimination, by comparing the performance of two different flows. DiffProbe's inventors created ShaperProbe (see earlier in this table), but ShaperProbe only allows the detection of throughput limitations, not delay and loss differentiation.
ChkDiff[105]	Concept	ChkDiff is a proposed method for detecting traffic differentiation at the application level. It will aim to identify whether any differentiation method is being used in the network (although does not specify the procedure used to differentiate the traffic).	To evaluate whether an access ISP is performing any differentiation in the upstream, ChkDiff will use the RTT metric between the user and a router on the access ISP's side. To detect downstream differentiation, ChkDiff will use the one-way delay between a measurement server and the end user.
Network tomography	Concept	Network tomography is a proposed technique to monitor the performance of a network in real-time. It has not yet been implemented, but simulations have been performed.	The development of network tomography is mainly focused on detecting loss and delay management.

103 See http://david.choffnes.com/pubs/differentiation-SIGCOMM2014Abstract.pdf
104 See http://ieeexplore.ieee.org/document/5461983/
105 See http://conferences.sigcomm.org/co-next/2012/eproceedings/student/p57.pdf