Nooren, Pieter; Prins, Mark

**Conference Paper**

# Transparency about net neutrality: A translation of the new European rules into a multi-stakeholder model

22nd European Regional Conference of the International Telecommunications Society (ITS): "Innovative ICT Applications - Emerging Regulatory, Economic and Policy Issues", Budapest, Hungary, 18th-21st September, 2011

**Provided in Cooperation with:**

International Telecommunications Society (ITS)

*Suggested Citation:* Nooren, Pieter; Prins, Mark (2011) : Transparency about net neutrality: A translation of the new European rules into a multi-stakeholder model, 22nd European Regional Conference of the International Telecommunications Society (ITS): "Innovative ICT Applications - Emerging Regulatory, Economic and Policy Issues", Budapest, Hungary, 18th-21st September, 2011, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/52189

**22nd European Regional ITS Conference**
**Budapest, 18-21 September, 2011**

**Pieter Nooren and Mark Prins**

# Transparency about Net Neutrality – a Translation of the New European Rules into a Multi-Stakeholder Model

## Abstract

The new European framework directive contains a number of policy objectives in the area of net neutrality. In support of these objectives, the universal service directive includes a transparency obligation for ISPs. This paper proposes a multi-stakeholder model for the implementation of this transparency obligation. The model is a multi-stakeholder model in the sense that it treats the content and form of the transparent information in close connection with the parties involved in the provision of the information and the processes in which they take part. Another crucial property of the model is that it distinguishes between technical and user-friendly information. This distinction makes it possible to limit the obligation to ISPs to the information for which they are in the best position to provide: the technical information on the traffic management measures that they apply, e.g., which traffic streams are subject to special treatment? Which measures are applied and when? The public availability of this technical information creates the opportunity for the other parties in the model to step in and contribute to the formulation of the user-friendly information for end users: which applications and services receive special treatment? When is their effect noticeable? It is expected that the involvement of other parties will lead to multiple, complementary routes for the formulation of the user-friendly information. Thus, the user-friendly information emerges in ways driven by market players and stakeholders that would be difficult to design and lay down in advance in the transparency obligation.

**JEL codes:** L15, L96, L98, O38
**Keywords:** net neutrality, transparency, traffic management

**Address:** TNO, P.O. Box 5050, 2600 GB Delft, The Netherlands
**E-mail:** pieter.nooren@tno.nl (corresponding author), mark.prins@tno.nl

# Contents

# 1 Introduction

## *1.1 Net neutrality and the role of transparency*

Net neutrality has, for a number of years, been a topic of often heated discussion in the Internet and telecom community. The crux of the issue is the extent to which different types of traffic on the Internet may be treated differently. This different treatment can take various forms. In one approach, so-called traffic management methods are used to prioritise, throttle or even completely block selected traffic flows. Another form of different treatment relates to the tariffs: the application of specific tariffs for traffic flows of selected applications or services carried over the Internet. Regardless of the characteristics of the different treatments that are applied, there can be concerns about the consequences for the open access of end users to the applications and services on the Internet.

In the US, the FCC made its first statements on net neutrality in 2004 [1]. The discussion has been ongoing ever since. Last year, the discussion in the US intensified with the joint Google-Verizon proposal [2] and the FCC's Open Internet ruling [3]. Regulators in other countries have held consultations on net neutrality and published guidelines and positions as well ([4],[5],[6],[7]).

The 2009 European framework directive [8] contains a number of policy objectives in the area of net neutrality as well. It is a subject that is clearly on the agenda of the EC, also in the context of its digital agenda for Europe ([9],[10],[11]). In support of its policy objectives, the universal service directive [12] includes a transparency obligation for ISPs. The purpose of this transparency is to give end users a meaningful insight into the traffic management methods which are employed by ISPs and what consequences they have for them. As explained above, the traffic management methods can have consequences for the access that end users have to services and for the service quality that they experience. Based on the information on traffic management that is provided to them, end users can make an informed choice between different ISPs offering Internet access services. Users can also decide to move to another ISP if they feel that the traffic management methods of their current ISP do not meet their needs. In this way, the transparency obligation can influence the ways in which the ISPs apply traffic management in their networks.

Each EU Members State has to decide on the best way to implement the European transparency obligation in more detailed regulation at the national level. This overall question has two components:

1. What are the basic principles for the transparency? These principles determine the scope of the transparency obligation, e.g. is an obligation appropriate for both fixed and mobile services? For both residential and business services?
2. Which technical and non-technical parameters should be made transparent? The question here is which information and form best contribute to the desired influence on ISPs.

These questions have been analysed at the request of the Dutch Ministry for Economic Affairs, Agriculture and Innovation to support them in their implementation of the transparency obligation in Dutch telecommunication regulations. The answers to these questions have been used to develop a comprehensive model for providing transparency that addresses both the principles and the relevant parameters for the transparency. This transparency model is the main subject of this paper. After the introduction of three illustrative use cases in Section 2, Section 3 discusses the basic principles and scope for the transparency provided by the model. Section 4 analyses the parameters to be made transparent, in combination with the stakeholders and processes involved. The paper closes with a number of concluding remarks in Section 5. We will also briefly discuss a parallel development in the area of net neutrality in the Netherlands. Recently, the Dutch parliament discussed and introduced explicit requirements for net neutrality in the new Dutch telecommunications law [13]. These new rules for ISPs complement the transparency obligation that has led to the formulation of the model outlined in this paper.

### *1.2 Research approach*

An extensive desk research has led to five representative use cases that capture the most relevant characteristics of traffic management measures that affect net neutrality. Three of these use cases are introduced in the next section. Further desk research into the traffic management measures and the information that is relevant to be made transparent has led us to the main characteristics of the transparency model. The crux of the model is that it is a multi-stakeholder model, with roles for ISPs, content providers, consumer interest groups, experts from the Internet community and the telecom regulator. These stakeholders have been closely involved through workshops and their contributions have been used in the development of the model. This ensures that proper attention has been given to the non-technical and organisational aspects of the model.

# 2 Three use cases for illustration

This section introduces three use cases that are used later on in this paper to illustrate the analysis that leads to the formulation of the transparency model. The use cases provide examples of how traffic management measures employed by ISPs can influence the end user experience and access to services and applications on the Internet.

### *2.1 Use case 1: Efficient distribution of streaming video*

Streaming video represents a growing part of the traffic on ISP networks. Streaming video is also sensitive to delays and various other irregularities in the network. The introduction of so-called caches in ISP networks (Figure 1) provides a way to both improve the quality of streaming video for the end user and to reduce the amount of bandwidth required to deliver the videos. The caches are used to store popular videos closer to the end customers. If the customer requests a cached video, the transmission path through the network can be shorter than in the situation without caching. Moreover, multiple customers can be served from one cached copy of the video, removing the need to transport the video all the way through the network for each individual customer. Caching is an important technical component of so-called Content Delivery Networks (CDNs [15],[16]). For end users, the use of CDNs by ISPs means that they can experience certain popular videos in a higher quality than other, less popular videos.

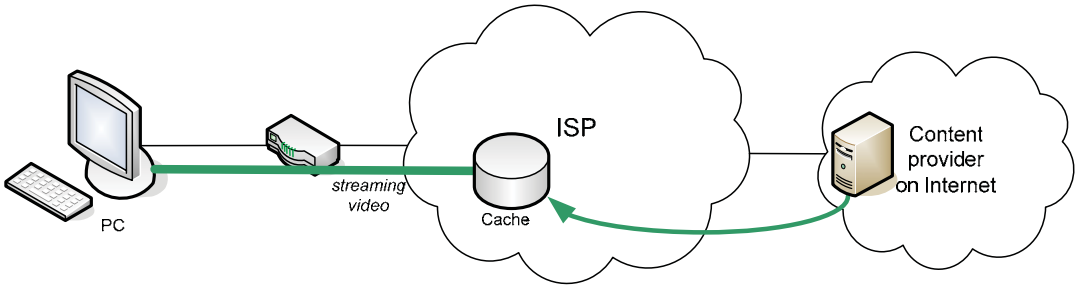


Figure 1: Efficient delivery of streaming video.

### *2.2 Use case 2: Blocking of VoIP traffic on mobile networks*

Over the last years, a number of cases have appeared in which end users could not use VoIP applications over their mobile Internet connection. Some of these cases revolved around (plans for) the detection and blocking of VoIP traffic in the ISP network (option a in Figure 2). Another well-known case that existed for some time is the inability to use Skype on iPhones over mobile networks.

Initially, the Skype application available for iPhones supported VoIP calls over Wireless LAN networks, but not over mobile networks (option b in Figure 2). For some time now, a version of Skype has been available in the Apple app store that does support VoIP calls over mobile networks [17].

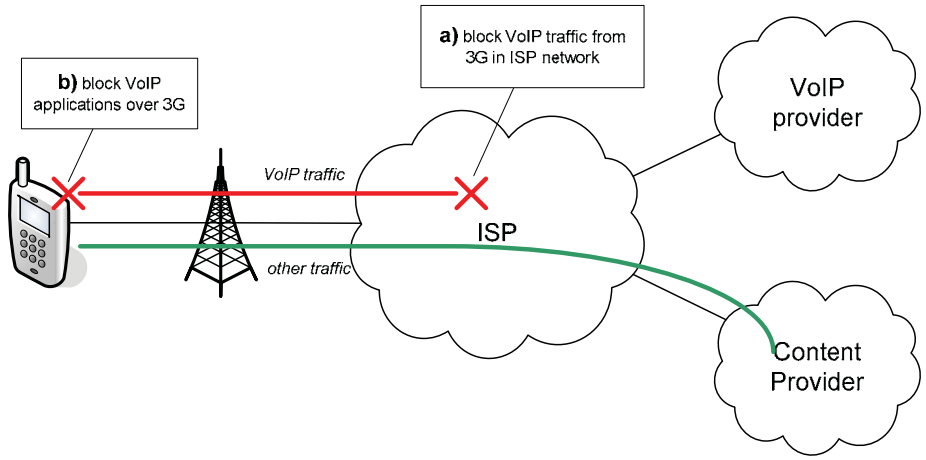


Figure 2. Two methods for blocking of VoIP traffic: a) blocking in the ISP network and b) blocking through the application on the mobile terminal.

### *2.3 Use case 3: Priority for time-critical applications during congestion*

Figure 3 sketches a traffic management measure that mobile operators can take during congestion in the radio network. It aims at reducing the impact of a temporary lack of capacity on the end user quality of experience. This is achieved by giving priority to services that are relatively time critical and therefore suffer most from congestion, at the cost of less time-critical services. Examples of time-critical services are VoIP, videoconferencing and webbrowsing. E-mail is a typical example of an application that is not time critical.

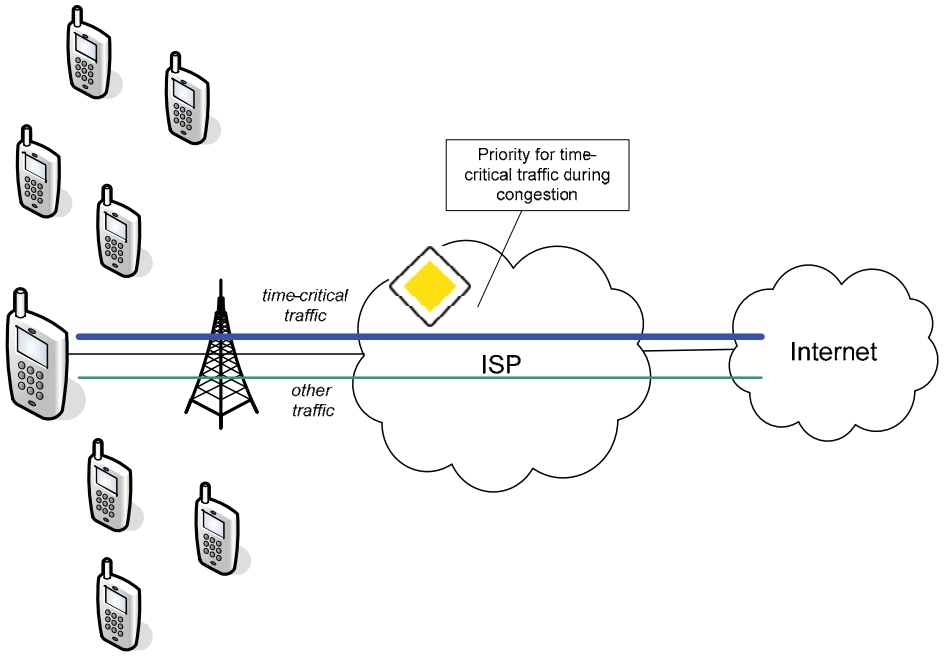


Figure 3. Priority for time-critical applications during congestion.

# 3 Basic principles and scope for transparency

This section analyses the basic principles for the desired transparency on traffic management measures. These principles determine the scope of the transparency obligation, e.g. is an obligation appropriate for both fixed and mobile services? For both residential and business services? These principles and scope are partly defined in the universal service directive and telecommunication laws in EU Member States, but some further development is needed for the actual implementation of the obligation.

## *3.1 Dimension 1: domain under control or influence of ISP*

The provision of broadband Internet services generally involves a chain of networks, see Figure 4. Different networks in the chain can be provided by different providers, who can each use their own traffic management methods. The universal service directive aims to provide end users with information on the traffic management methods employed by their own ISP. It seems logical to limit the transparency obligation for ISPs to the parts of the network chain that they control themselves, or where they have significant influence.

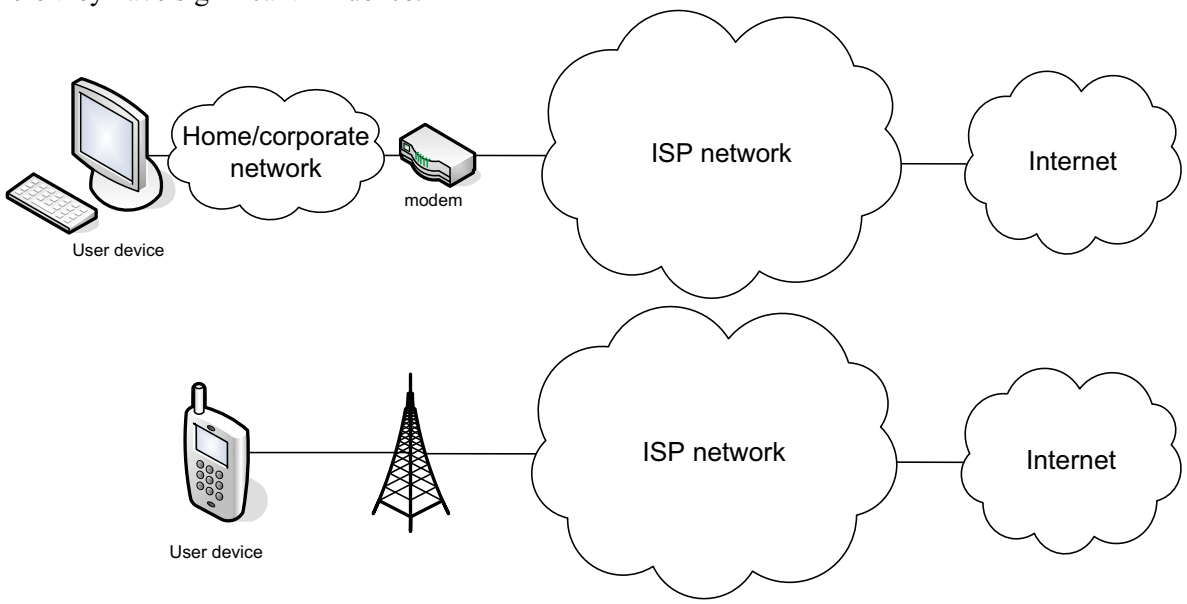


Figure 4. The IP network chain involved in the provision of broadband Internet in typical fixed networks (top) and mobile networks (bottom).

- ISPs have full control over the traffic management measures they take in their own network. This control extends from the delivery point at the end user, e.g. on a broadband modem or a mobile terminal, to the connection between the ISP network and the public Internet. The transparency obligation for ISPs clearly applies to this part of the network chain.
- ISPs generally have no control or influence over the IP networks and servers that make up the public Internet. This part of the network chain is therefore outside the scope of the transparency obligation.
- The management of the home or corporate network is typically done by the end user and therefore not under control of the ISP. However, an ISP can still have a substantial influence on the traffic management in this part of the network chain, for example by prescribing the use of specific modems or terminals, or by prescribing or forcing the use of specific settings on such equipment. In this context, the universal service directive mentions "*any restrictions imposed by the provider on the use of terminal equipment supplied*" in article 20(1)(b). This type of influence of the ISP plays a role in variant b) of the use case "blocking of VoIP traffic on mobile networks" in section 2.2. In this variant, the mobile ISP chooses to provide the end

user with a mobile terminal that does not support the use of VoIP over the mobile network. Thus, the mobile operator has an influence on the traffic management measures in the terminal through his selection of the terminal he provides. These traffic management measures are therefore within the scope of the transparency obligation.

### *3.2 Dimension 2: for ISPs providing fixed services and for ISPs providing mobile services*

The universal service directive does not distinguish between fixed and mobile services in its formulation of the transparency obligation. Moreover, examples of traffic management measures that limit the access to applications and services on the Internet are known for both fixed and mobile networks. In fixed networks, a number of examples are in the area of blocking or throttling peer-to-peer (P2P) filesharing traffic ([18],[19],[20],[21]). In mobile (UMTS/3G) networks, a number of cases of VoIP blocking are known, along the lines of the use case described in section 2.2. It is therefore appropriate to apply the transparency obligation to both ISPs providing *fixed* Internet access services and to ISPs providing *mobile* Internet access services.

### *3.3 Dimension 3: for ISPs providing services to consumers and for ISPs providing services to businesses*

Transparent information on traffic management measures is of interest to both consumers and business end users. Both groups can benefit from the availability of this information, as they are in a better position to make a choice between the Internet access offerings from different ISPs. It is therefore appropriate to apply the transparency obligation to ISPs providing services to consumers and to ISPs providing services to business users. A separate report ([22], in Dutch) provides some additional analysis and remarks on the provision of transparent information in the business market.

### *3.4 Dimension 4: effect of managed services on Internet access service*

Initially, the net neutrality discussions focused at the different treatment of traffic flows in the public Internet. The public Internet is a global system of interconnected networks that use the IP protocol to transport data between the connected end points. The adjective “public” in public Internet emphasises that end users can access all information and applications on the global Internet from their own end point. This information and the applications are offered, either for free or against a payment, by content providers that are connected to an Internet end point themselves as well. The role of the public Internet is essentially that of a transport network that connects users and application providers across the globe. In principle, it can support all IP-based services and applications by transporting IP traffic between application providers and users worldwide. ISPs play an important role in the public Internet, as they provide the Internet access service: the part of the Internet transport chain between the home network or mobile terminal of the user and the Internet core (see Figure 4). In general, the Internet access service is a best-effort service, e.g., there are no guarantees that IP packets sent over the network reach their destination end point within a certain time. This type of best-effort Internet access services matches the best-effort characteristics of the Internet core.

Providers of Internet access services increasingly provide other IP-based services in parallel with the Internet access service over the same infrastructure. Two well-known examples here are IPTV and IP telephony services provided by a range of European ISPs over their DSL, cable and fibre access networks. Although these services are delivered over the same network infrastructure as the Internet access service, they are in a number of respects separate from the Internet access service. Often, these services are called “managed services” [9]. Other terms that are used are “specialized services” [3] and

"additional, differentiated online services"[2] The adjective "managed" can be slightly misleading here, as it does not provide a clear demarcation from the public Internet access service. Although the Internet access service and the Internet core are characterized as best effort, they are subject to various types of management to ensure their efficient and reliable operation. Apart from this, application and service providers on the Internet actively monitor and manage their web servers, app stores and other resources. Nonetheless, the degree of management and guarantees for managed services is typically higher than for the best-effort public Internet.

The co-existence of (services and applications over) the public Internet and managed services leads to the emergence of the so-called two-lane model [21]. In the two-lane model, the broadband access connection of an end user is used to provide him both with the Internet access service and a number of managed services, see Figure 5.

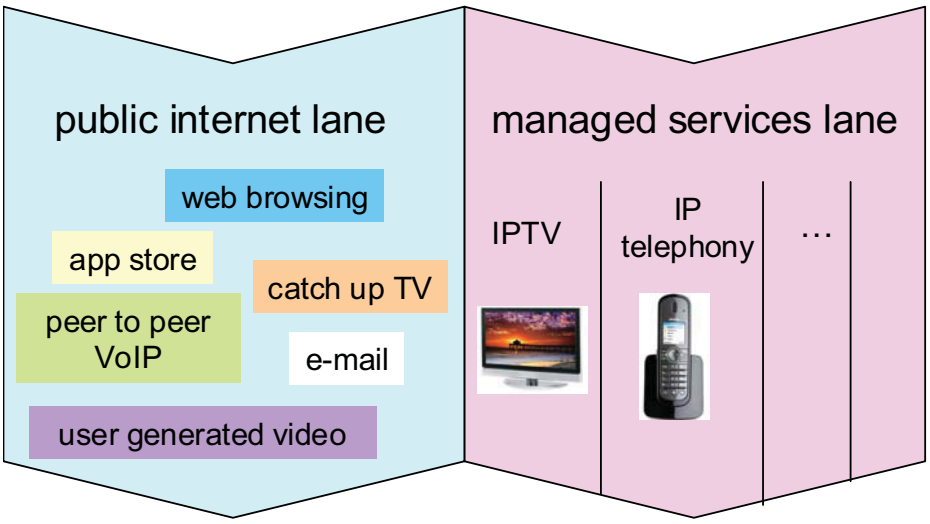


Figure 5. Two-lane model with Internet access service and managed services provided over a single broadband access.

In the public Internet lane, the ISP provides an Internet access service to the end user. Through this access service, the user gains access to the information and applications on the public Internet. Thus, the user has access to a very large variety of information and applications on the Internet, while he only buys the Internet access service from his ISP. In a number of cases, the end user is likely to enter into an agreement or contract with a content provider on the public Internet. These agreements do not involve the ISP and also do not require any action from the ISP. In the managed services lane, the ISP has an agreement with the end user to provide him specific services. There can be a single agreement, made directly between the ISP and the end user. There can also be multiple, interrelated agreements, e.g. one agreement between the end user and a content provider, in combination with a second, related agreement between the content provider and the ISP. Each specific service that an end user buys in the managed services lane requires, in principle, an action by the ISP. Typically, part of this action consists of taking measures to guarantee the quality of the service, for example through the reservation of dedicated bandwidth. In the public Internet lane, no measures are taken to guarantee the quality of specific services. Table 1 summarizes the characteristics of the public Internet lane and the managed services lane.

Table 1. Characteristics of the public Internet lane and the managed services lane.

| | **public Internet lane** | **managed services lane** |
|---|---|---|
| **Services provided by ISP** | Single service: access to the global public Internet | Specific services, e.g. IPTV, IP telephony, … |
| **Services provided by other providers** | All services on the public Internet ("Over the Top" services) | Specific services, subject to agreement between other provider and ISP |
| **Agreements between ISP and end user** | Single agreement covering Internet access service | Individual agreements per service |
| **Quality** | Best effort (good but no guarantees) | Typically with statistically guaranteed quality for each service |

Initially, the net neutrality discussion was confined to the public Internet lane. With the introduction and rise of the managed services, the discussion widens itself to both lanes ([9],[3]). The universal service directive mentions "*information on any other conditions limiting access to and/or use of services and applications*" and thus does not make a distinction between the two lanes. Nevertheless, in the further implementation of the transparency obligation, it does seem appropriate to distinguish between the two lanes. In particular, it is probably useful to limit the extent of the obligation for the managed services lane. After all, end users already expect a number of specific features and limitations from services in the managed services lane. In an IPTV service, for example, an end user typically already expects a specific, guaranteed quality (standard definition or high definition) and access to the TV channels specified in the IPTV subscription. Such features and limitations have been agreed between the end user and the ISP at the time the end user purchased the service. A transparency obligation for ISPs for the traffic management measures that they use in the provision of their managed services has little added value for the end user and is therefore not appropriate. Thus, ISPs doe not need to be transparent about the measures they take to guarantee the quality of their IP telephony service in their managed services lane. Similarly, they do not need to be transparent to end users about the measures they take to give 112 emergency calls priority over regular calls.

At the same time, the provision of managed services can affect the quality of services over the public Internet lane. In many cases, the Internet access service and the managed services are delivered over a single broadband infrastructure, sharing the available capacity. ISPs that provide guaranteed capacity (e.g., bandwidth) to their managed services in order to guarantee their quality thus typically decrease the capacity available for the services and applications delivered over the public Internet lane. Managed services can therefore negatively affect the quality of services that end users receive over the public Internet lane. This influence is relevant for end users in their choice between ISPs that offer combinations of managed services and public Internet access. If such an influence of the managed services on the capacity or performance of the public Internet lane exists, it is useful that the end user is made aware of this. Summarising, a transparency obligation for ISPs is appropriate for the traffic management measures that they take in the Internet access service and for the effect that the managed services they provide have on the Internet access service.

### *3.5 Dimension 5: distinction between traffic flows within the Internet access service.*

In the net neutrality context used in this paper, not all traffic management measures applied in the public Internet lane are within scope of the transparency obligation. Transparency is only required if there are traffic management measures that treat different traffic flows in different ways. Thus, no transparency is required about measures that affect the combined traffic flow without distinction

between the smaller flows that make up the full flow. As an example, so-called traffic concentration occurs in multiple locations in most ISP networks, see Figure 6.

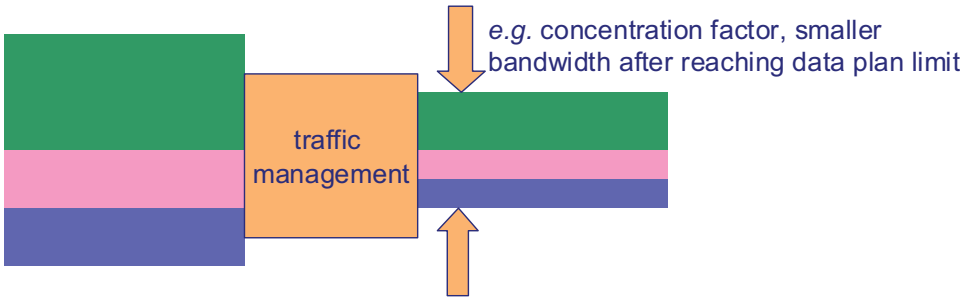


Figure 6. Traffic management measure that treats all traffic flows equally.

The bandwidth available for the aggregated traffic flow is smaller than the sum of the bandwidths available on the individual customer connections. The concentration typically does not distinguish between traffic flows: if needed, all traffic flows are throttled with the same factor to meet the maximum bandwidth available for the aggregate flow. Another example of a traffic measurement measure that does not distinguish between different traffic flows is an enforced bandwidth reduction for customers that have reached the maximum amount of data that they have available in a Fair Use Policy (FUP). For these types of traffic management, a transparency obligation in the context of net neutrality is not appropriate.

A transparency obligation is appropriate when a traffic management measure does treat different traffic flows within the Internet access service differently, see Figure 7. For example, the different treatment can consist of the rerouting a specific stream (as in the streaming video use case in section 2.1), or the blocking of a specific flow (as in the VoIP blocking use case in section 2.2).

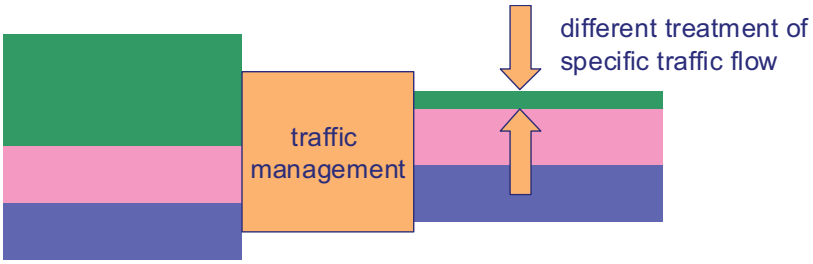


Figure 7. Traffic management measure that treats a specific traffic flow differently.

Summarising, a transparency obligation for ISPs is appropriate for traffic management measures that lead to a different treatment of traffic flows within the Internet access service. Measures that only affect the full traffic flow should not be subject to the transparency obligation analysed in this report.

# 4 Transparent information, stakeholders and processes

## *4.1 Requirements for the model*

Transparency about traffic management measures means that ISPs provide information to the public on the technical measures they apply in their networks that treat different traffic flows in different ways. There are many options for the content, form and extent of this information. This section analyses which content and form best contribute to the desired effect of the transparency obligation, i.e. influencing the ways in which the ISPs apply traffic management in their networks, while at the same time meeting a number of other criteria, such as future proofness, the ability to enforce the

obligation and limited costs for the parties involved. This shows that it is necessary to analyse the content and form of the information in close connection with the parties involved in the provision of the information and the processes in which they take part. In the remainder of this paper, the term transparency model is used for the combination of the information itself, the parties and the processes.

The main requirement for the model is that it is effective: the combination of information, parties and processes must lead to the desired influence on the traffic management measures applied by ISPs. Apart from this main requirement, there are a number of additional requirements from the universal service directive, telecommunication laws and a number of wishes from market parties and stakeholders, such as ISPs, content providers and consumer interest groups.

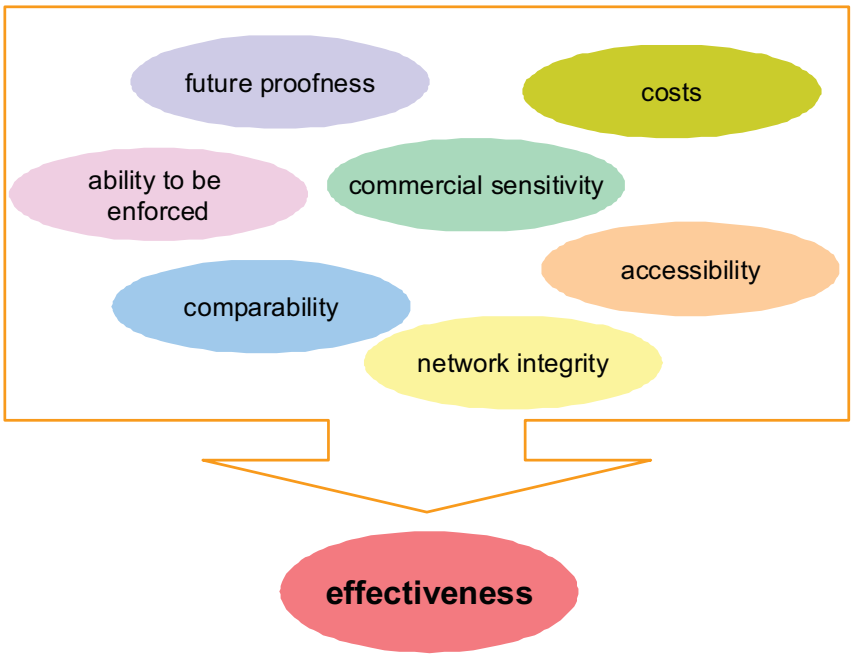


Figure 8. Requirements and criteria for the transparency model.

Figure 8 provides an overview of the requirements considered during the development of the model.

- Future proofness is important, as the model and the regulations in which the transparency obligation is laid down must be able to cope with the rapid developments in services and applications, networks and traffic management methods. It is in the interest of market parties, end users and other stakeholders that the rules governing the transparency are stable and predictable over a longer period of time.
- The ability to be enforced contributes to the effectiveness of the transparency obligation. It is to be expected that regulators, such as the Dutch telecom regulator OPTA, will be involved in the enforcement of the obligation. Other parties and the Internet community in general can play a role in the enforcement by pointing out potential problems. For a proper enforcement, it is necessary that regulators have sufficient and clear information available on the traffic management measures.
- Comparability between traffic management information from different ISPs is needed to enable end users to properly weigh the different offerings and select the one that fits their needs best.
- Accessibility of the information is important for its effectiveness. Various types of accessibility are needed :
    - The information must be easy to find on ISP websites and other ISP publications.
    - The information must be understandable. Here, it is important to note that information that is understandable for technical experts is probably not understandable for most consumers. Conversely, information understandable for consumers may not properly address the information needs of a technical expert.

- Commercial sensitivity calls for a balance between the interests of ISPs and the other stakeholders. The goal of the transparency requirement is to achieve an influencing of the ISPs use of traffic management measures. It can very well be that with the introduction of the transparency obligation, traffic management becomes a new area in which ISPs compete to attract end users. This is a desired effect of the obligation. However, if ISPs are required to disclose very detailed information on the traffic management measures they use, a situation can arise in which ISPs get an unnecessary deep insight in the dimensioning and operations of their competitors' networks. This is clearly not the intent of the transparency obligation.
- Network integrity is another point requiring attention. It is also linked to the level of detail in the information that is requested from the ISPs. A high level of detail in the information can point malicious parties to potential vulnerabilities in networks and services.
- The costs of the provision of transparent information by the ISPs, for the enforcement of the obligation by the regulator and the costs for other stakeholders are also important.

The above list of requirements has been used to develop the transparency model described in the following sections. Feedback and suggestions from two workshops with representatives from ISPs, content providers, consumer interest groups, experts from the Internet community and regulator OPTA have been used in its development.

## *4.2 Main features of the transparency model*

### *4.2.1 Technical and user-friendly information*

The requirements for the transparency model and the desired information on traffic management are quite diverse in nature. It is therefore difficult to meet all requirements with a single type of information. The model proposed here therefore contains two types of information, aimed at different audiences: technical information and user-friendly information.

- The *technical information* describes the traffic management measures that the ISP takes in technical terms. The objective of this information is to provide experts with an access to the actual technical measures. The technical information is probably not very useful for mainstream end users.
- The *user-friendly information* describes the consequences of traffic management measures for end users, in terms that can be understood by a wide audience of users.

The split between technical and user-friendly information is thus made from the perspective of a mainstream end user who will have difficulty to interpret the technical information. Technical experts will probably find the technical information to be user friendly as well.

Figure 9 sketches the main features of the transparency model with these two categories of information. The technical information provides the basis for the model and is subsequently translated into user-friendly information.

For each traffic management measure that falls within the scope defined in section 3, the technical information provides the following information elements:

1. Which traffic stream is subject to a special treatment through traffic management measures?
2. Which measures are applied to this traffic stream?
3. When are these measures applied?

Section 4.3 examines the optimal level of detail and the precise types of information for these three elements.

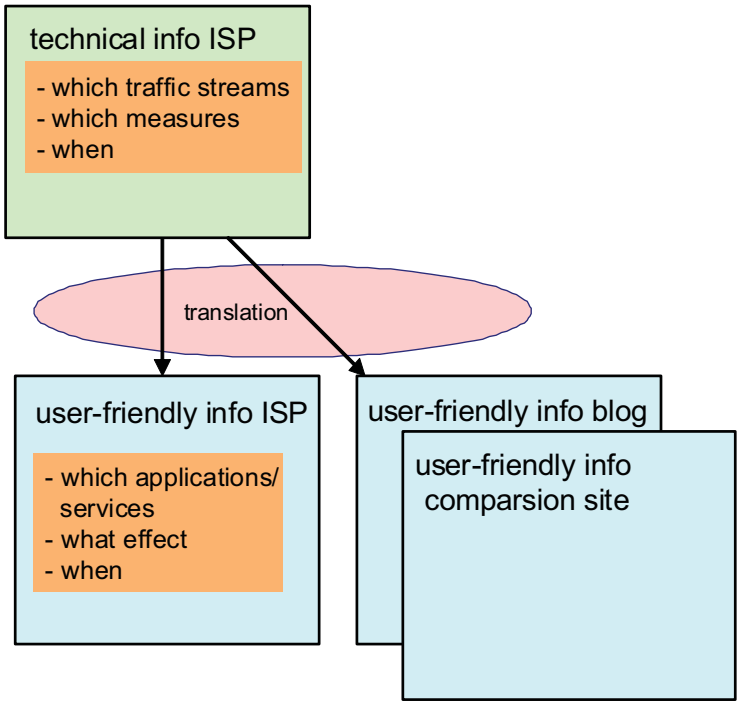


Figure 9. Transparency model with technical and user-friendly information.

The technical information is of direct value for experts that want to analyse ISP traffic management measures. Apart from this, the technical information is the starting point for the formulation of user-friendly information, potentially but not necessarily by the same experts. ISPs are by far in the best position to provide the technical information on the traffic management measures that they apply. Given the key role of the technical information, it is proposed here to oblige the ISPs to provide the technical information on the traffic management measures they apply. Including the above three elements in the obligation also makes it possible to compare the traffic measurement methods of different ISPs at the technical level.

The *user-friendly information* is derived by translating the technical information into its effect on the end user experience, in terms that can be understood by a wide audience of users. Here, the answers to the following three questions are relevant:

1. Which applications and services receive special treatment from traffic management?
2. What is the effect of the traffic management measures on the services experienced by end users?
3. When is this effect noticeable?

As explained in section 4.4, the translation of the technical information into answers to these questions is relatively straightforward but also partly subjective. This is one of the considerations that have led to the proposal not to introduce an obligation for ISPs to provide user-friendly information.

### *4.2.2 Roles for market parties and other stakeholders*

Just as important as the technical and user-friendly information in the model are the roles that ISPs and other stakeholders have in the formulation, interpretation, translation and checking of the information. Figure 10 provides an overview of the interaction of a number of relevant market parties and other stakeholders in the model.

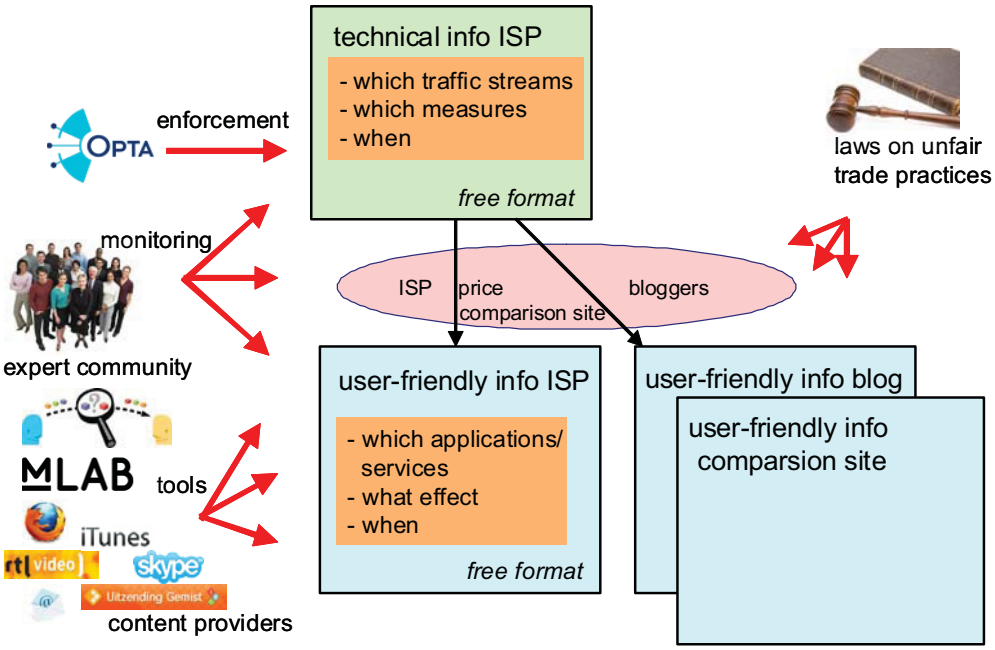


Figure 10. Roles for ISPs and other stakeholders in the transparency model.

- ISPs obviously play a key role in the model. They have an obligation to provide technical information on the traffic management measures they take, to the extent that they are within the scope defined in section 3. Apart from providing this obligatory information, ISPs will probably be inclined to explain the technical information to their (potential) customers by translating it to user-friendly information.
- The public availability of the technical information from the ISPs also enables other parties, such as comparison sites, to publish this information on their own websites and, as an option, to make their own translation to user-friendly information. As a result, end users may have different sources of user-friendly information available. Since the user-friendly information is inherently somewhat subjective, there can be different views and discussions on the correctness of the translation that leads to the user-friendly information. In itself, such discussions on the effect of traffic management on the end-user experience are not problematic. They can serve to generate more attention among the public for net neutrality issues and the role of ISP traffic management. In this way, such discussions contribute to the desired effect of the transparency obligation: influencing the traffic management measures applied by ISPs. Market parties and stakeholders who feel that information published by others is damaging can seek to correct this through the existing laws on unfair trade practices.
- It is foreseen that the regulator will have a role in the enforcement of the obligation. This enforcement will focus at the correctness and completeness of the technical information that the ISPs are obliged to provide. As discussed in section 4.4, the derivation of most of the user-friendly information from the technical information is relatively straightforward but also partly subjective. It is therefore not envisaged that the regulator will also enforce the correctness of the subjective information. This is also an important consideration for the proposal not to introduce an obligation for the provision of user-friendly information, as this would lead to an obligation that would be difficult to enforce. As described in section 4.4, there are also other reasons for not introducing an obligation for the provision of user-friendly information.
- The expert community on the Internet closely follows the national and international developments in networks and services. Experts from the community can analyse, compare, and comment on the technical information provided by ISPs and also translate it to user-friendly information. This information from experts can become available to a wide audience through forums and weblogs. With publicly available tools such as M-lab [23], experts can also check the correctness and completeness of the technical information provided by the ISPs.

- Price comparison sites can also analyse the available technical information, translate it to user-friendly information and include it in their comparison tables. For many end users, price comparison sites are an important source of information that they consult when choosing between different Internet access service offerings.
- Content and application providers on the Internet can also study and check the technical information provided by the ISPs. They may also want to translate and explain the consequences of the ISP traffic management measures to their own end users.

## *4.3 Technical information*

The technical information describes the traffic management measures that the ISP takes in technical terms. The objective of this information is to provide experts with an access to the actual technical measures. The technical information is made up of the three elements mentioned earlier ("which traffic", "which measure" and "when"). The following sections analyse in detail what the specific content of each element should be.

### *4.3.1 Which traffic*

The challenge in the formulation of the transparency obligation for the "which traffic" element is to determine the optimal level of technical detail, which is not necessarily the same as the maximum level of detail. The proposal is to oblige the ISPs to provide a description of the traffic streams in terms of:

> **Description A:** *Traffic flows from (classes of)* ***applications*** *including the list of (combinations of)* ***technical parameters*** *that characterise the traffic, such as URL, domain name, IP address, protocol, port number, AS number, peering partners, terminal types, …*

Thus, the technical parameters that are used to distinguish specific traffic flows need to be mentioned, but not the actual values of the parameters. For the three use cases from section 2, the technical information according to this obligation could be, for example,

- Efficient distribution of streaming video: *"streaming video traffic containing popular content from selected Internet service providers determined by the URL of their website"*
- Blocking of VoIP traffic on mobile networks:
  - option a)*"VoIP traffic over the mobile network, characterised by different combinations of the IP destination address and the use of the SIP protocol"*
  - option b) *"VoIP traffic over the mobile network, characterised by the combination of the use of selected applications on the mobile terminal and a mobile network connection"*
- Priority for time-critical applications during congestion: *"real-time and interactive traffic, characterised by the use of the HTTP, SIP or RTP protocol"*

In general, this level of detail is the minimum level required by experts to determine which traffic flows are affected by traffic management measures and which flows are not. If the ***technical parameters*** part is removed, it is no longer possible to make the distinction between the traffic management options a) and b) in the VoIP blocking use case. In the third use case, it would be unclear which traffic flows would be in the category real-time and interactive traffic. Thus, without this information it is not possible for technical experts to properly examine the extent of the traffic management measures and to make a proper translation to user-friendly information.

The technical parameters part is also needed for effective enforcement of the transparency obligation. Part of the enforcement activities will be driven by complaints of end users who suspect that the performance of certain applications is negatively affected by ISP traffic management measures. Without the information on the technical parameters involved, it is difficult for the regulator to assess

whether an application is affected by a published traffic management measure, or whether it is affected by another measure that has not been published.

For ISPs, the level of detail that is created by publishing information on the technical parameters can also be useful, as it enables them to better describe the extent and scope of their measures. Without information on the technical parameters, it could appear that a measure affects wide classes of applications, while it actually only affects a smaller group of applications.

A description containing significant more detail that has been considered in this study, but that is not proposed to be part of the transparency obligation is:

> **Description B:** *Traffic flows from (classes of)* ***applications*** *including the list of (combinations of)* ***technical parameters*** *that characterise the traffic, such as URL, domain name, IP address, protocol, port number, AS number, peering partners, terminal types, …and the* ***specific values of the parameters*** *that characterise the traffic.*

For the three use cases, the technical information according to this more detailed description could be, for example,

- Efficient distribution of streaming video: *"streaming video traffic containing popular content from selected Internet service providers determined by the URL of their website. The URLs concerned are uitzendingengemist.be, thevideoarchiver.net en nationalevideo.nl."*
- Blocking of VoIP traffic on mobile networks:
  - option a)*"VoIP traffic over the mobile network, characterised by different combinations of the IP destination address and the use of the SIP protocol. As of September 15, 2011, the list of IP addresses is 192.168.31.4, 192.168.31.5, 192.168.20.0/24, 172.16.4.54, 172.16.4.55, 172.16.7.145, 172.16.7.231, 10.3.234.4, 10.67.45.123, 10.23.98.215, 10.1.34.2, 192.168.34.2, 10.76.0.0/28, 172.19.45.201, 172.19.45.202, 10.2.80.31, 10.2.80.131, 10.2.80.231."*
  - option b) *"VoIP traffic over the mobile network, characterised by the combination of the use of selected applications on the mobile terminal and a mobile network connection. As of November 1, 2011, the applications affected are VoIPXpress, Zceip, InetPhone, Speakerz, VoiceXpresser."*
- Priority for time-critical applications during congestion: *"real-time and interactive traffic, characterised by the use of the HTTP, SIP or RTP protocol"*

The underlined sentences are the additions compared to the less detailed description A introduced earlier. Note that in the third use case, parameter values do not play a role. Therefore description B does not add information in this specific case.

With the description B information, technical experts can check in detail whether the information provided by the ISPs is correct and complete. Also for the enforcement by the regulator, the description B information can be valuable in situations that require a detailed analysis of traffic management measures. At the same time, it is questionable whether the additional information in description B will contribute to better or more complete information for the mainstream end user. The contribution of the additional information to the effectiveness of the transparency obligation, which is largely determined by the user-friendly information, is therefore in most cases limited.

For ISPs, the publishing and updating of the description B information would require substantially more effort than is required for description A. Furthermore, the publication of the description B information would potentially disclose substantial amounts of information on the dimensioning and operations of the ISP networks. It is not possible to make a generic assessment of whether the description B information is commercially sensitive or not, as this depends strongly on the specific

information. However, it is clear that commercial sensitivity and network integrity would require attention.

Given the limited contribution that is expected from the description B information to the overall effectiveness of the transparency obligation, the additional effort required from ISPs and the potential issues around commercial sensitivity and network integrity, this study does not propose to include the description B information in the transparency obligation towards ISPs.

As noted above, the description B information can be valuable in the enforcement of the transparency obligation. It is quite conceivable that an ISP would provide description B information to the regulator on a confidential basis in the context of a specific enforcement case. Here, the amount of information provided by the ISP can remain limited to the information needed by the regulator to perform its analysis of that specific case. The confidentiality can remove the concerns around the potential commercial sensitivity and network integrity issues.

Obviously, an ISP can still decide to make the description B information publicly available if he considers this useful in his explanation of a traffic management measure. For example, in the first use case on streaming video, the ISP can decide to publish the URLs of the video services involved. These URLs can be incorporated in the user-friendly information and provide additional insight to end users on the effect of the traffic management measure. For the ISP itself, it can also be useful to publish the list of involved URLs, for example to prevent speculations in the market on which video services receive special treatment and which services do not. This study proposes to leave the decision on the publishing of the description B information to the ISPs. Here, it can be expected that ISPs will also consider the questions that can arise among end users and other stakeholders as a result of the obligatory provision of the description A information.

#### *4.3.2 Which measure*

Apart from the characterisation of the traffic flows that are subject to specific traffic management measures, it is of course necessary to know what that the measure actually entails. This element of the technical information can be described as

> *The technical measures used to treat the involved traffic stream differently compared to other traffic streams in the Internet access service*

The description of the measure must be formulated in technical terms and, where possible, be quantified. There is a wide variety of options to implement traffic management measures in networks. In practice, most of them are within one of the following categories:

- Blocking the traffic stream, dropping or removing its packets. Here, a qualitative description is generally sufficient.
- Limiting the bandwidth available for a stream (“throttling”). Here, a quantitative description of amount of bandwidth involved is needed.
- Use of different priorities, for example those based on 3GPP QoS classes [24] or DiffServ code points [25]. In such situations, it is necessary to provide the assignment of traffic streams to the different classes.
- Routing over a separate part of the network. Here, it is needed to explain what this alternative routing entails and how it is different from the routing used for the other traffic streams.
- Rerouting to new destinations. This calls for a description of the new destination and an explanation how it is related to the original destination.
- Interference with the traffic stream itself. Here it should be made clear which changes are made in the traffic, for example by removing, adding and modifying specific packets.

For the three use cases, this information could look like this:

- Efficient distribution of streaming video: *"The streaming video is provided from caches within our own network instead of from the network of the video provider. As a result, the video is delivered over a shorter route. The video content itself is not affected."*
- Blocking of VoIP traffic on mobile networks:
    - option a) *"The involved traffic stream is blocked."*
    - option b) *"The involved applications on the mobile terminal do not allow VoIP sessions over mobile network connections."*
- Priority for time-critical applications during congestion: *"The involved traffic stream is assigned to the "streaming" QoS class and receives priority over the other streams that are assigned to the "background" class."*

### *4.3.3 When*

The third element of the technical information states when the traffic measurement measure is applied or active. This can simply be a specific time period during the day. An important category of measures is probably not applied during fixed time periods, but during specific situations such as congestion in the network. Combinations of specific situations and times are also possible, for example *"after exceeding the data limit of 10 Gigabytes per month"*. The information to be provided for the "when" element of the technical information can thus be described as

> *The time periods or specific situations during which the specified measures are applied to the specified traffic streams.*

For the three use cases, this information could look like this:

- Efficient distribution of streaming video: *"Always"*.
- Blocking of VoIP traffic on mobile networks, options a) and b): *"Always"*.
- Priority for time-critical applications during congestion: *"During congestion in specific cells in the mobile network"*.

### *4.3.4 Presentation of technical information*

The previous sections discuss the obligations for the content of the technical information. It could also be considered to introduce an obligation for the form and format used to publish the technical information. This study proposes not to prescribe specific forms or formats. The main consideration here is that there is a wide variety of potential traffic management measures that can affect a wide variety of (classes of) applications. It would be very difficult to come to a format that is useful and appropriate in all these cases, as can be seen from the use case examples in the previous sections. In addition, the requirement of future proofness implies that such a format would also need to be suitable for the description of future traffic management measures that are not yet known today.

Another reason not to prescribe a specific format is that this could limit the opportunities for ISPs to distinguish themselves from their competitors in the area of traffic management. In the Netherlands, this consideration has led to the prescribing of a number of obligatory information elements in combination with a free format in the implementation of a transparency obligation for telephony tariffs [26].

The free format allows ISPs to present the technical information in connection with the user-friendly information. This approach has already been used by a number of Canadian ISPs ([19],[20]) in their fulfilment of the Canadian transparency obligation for traffic management measures [7].

## *4.4 User-friendly information*

### *4.4.1 Subjective translation from technical information*

The user-friendly information is derived by translating the technical information into its effect on the end user experience. The essence of the user-friendly information is provided by the answers to the three questions from section 4.2.1. These answers are closely related to the three elements in the technical information that ISPs are obliged to provide:

1. Which applications and services receive special treatment from traffic management?
   The applications and services are determined by the selection of the traffic flows that are treated differently by traffic management.
2. What is the effect of the traffic management measures on the services as they are experienced by end users?
   The effect depends on the specific traffic management actions on the selected traffic flows.
3. When is this effect noticeable?
   The effect can be noticed when the traffic management measures are active.

This shows that to a large extent, this translation is relatively straightforward. At the same time, the translation is often subjective as there are also factors other than ISP traffic management measures that affect the end user experience. For example, there can be a strong influence of other networks in the IP network chain (Figure 4). Such factors can (partly) hide the effect of traffic management measures or, on the contrary, amplify their effect. Another source of subjectivity is that the end user experience also depends on the expectation of the service quality that an end user has formed before the actual use of the service. This expectation varies between end users. The translation from technical to user-friendly information and the subjectivity that plays a role is illustrated below for the video streaming use case. For the other two use cases, example translations are provided in a separate report ([22], in Dutch).

- *Which applications and services?* It is clear that video services can benefit from the traffic management measure. This information can already be useful for end users: depending on how often they watch streaming videos, the measure can influence their experience. As explained in section 4.3.1, an ISP can choose to also publish the URLs of the video services involved. It is straightforward to incorporate this additional information in the user-friendly information to provide a more detailed insight to the end users.
- *What effect?* It is difficult to make a generic statement on the effect for the end user experience. If the ISP network carries a large traffic load, the streams of the video services involved can be experienced with a higher quality than other video streams. This is because they have been cached and have a shorter network path to traverse, making them less vulnerable for congestion problems. On the other hand, if the overall network load is low, it is quite conceivable that the measure has a negligible effect on the user experience, as all video streams can be properly delivered. The interesting point of this specific traffic management measure is that improving the quality of the video services involved does not have to occur at the cost of other video services and the other Internet applications in general. On the contrary, the reduction of the overall network load achieved with the caching can improve the experience of the other services and applications, again dependent on the actual distribution of the traffic over the network.
- *When?* The answer to this question is simple: always.

### *4.4.2 No obligation for user-friendly information*

As explained in section 4.2.2, multiple parties are in a position to develop user-friendly information by translating the technical information that ISPs are obliged to publish: the ISPs themselves, but also technical experts from the Internet community, price comparison sites, consumer interest groups, content and application providers and others. This study proposes not to oblige ISPs to provide user-friendly information, for a number of reasons:

- Because the user-friendly information is derived through a partly subjective translation, it is difficult to formulate clear obligations on the content of the user-friendly information. Such an obligation would also be difficult to enforce, as there is no objective test available for the assessment of the information.
- An obligation also does not seem to be necessary. It is expected that the ISPs themselves will be inclined to translate the technical information into user-friendly information. This would be the best way for them to explain the technical information that they have to provide on a clearly visible part of their website to their (potential) customers.
- Apart from explaining the effect of their traffic management measures for their end users, ISPs will probably also want to explain why they take the measures. Up until now, traffic management measures have a certain negative connotation as they are known primarily from incidents in which they had negative consequences for end users. For ISPs, this can be a motivation to carefully explain why they take certain measures and how they balance the interests of end users and content providers with their own interests.

An argument in support of an obligation for ISPs to publish user-friendly information is that this would also provide the opportunity to make the information from different ISPs more comparable. However, because it is difficult to formulate objective requirements for the user-friendly information, it would be difficult to make this mechanism work in practice. In the model proposed here, the comparability can emerge via other routes. For example, price comparison sites can incorporate their interpretation of the ISP traffic management measures in their comparison tables and search tools for Internet access services. The authors of weblogs can comment on the traffic measurement measures they find important and compare the approaches used by different ISPs. Through these alternative routes, the user-friendly information thus emerges in ways driven by market players and stakeholders. This will probably not lead to a single approach or format used by all market parties and stakeholders. Different comparison sites and weblogs will tailor the content and presentation of their information to the audience they are targeting.

# 5 Concluding remarks

## *5.1 The multi-stakeholder transparency model proposed in this study*

The scope of the transparency obligation has been determined by a demarcation on five points. On at least one point, the influence of managed services, the demarcation is new or different from the demarcation proposed in other studies or initiatives. With the introduction and rise of the managed services, it is important to widen the analysis to both the public Internet lane and the managed services lane. Specifically, it is proposed to include the effect that the managed services have on the Internet access service in the scope of the obligation. This is an extension compared to traditional analyses in which only the effect of measures on traffic streams within the Internet access service is considered.

The transparency model itself that is proposed here treats the content and form of the information in close connection with the parties involved in the provision of the information and the processes in which they take part. Another crucial property of the model is that it distinguishes between technical and user-friendly information. This distinction makes it possible to limit the obligation to ISPs to the information for which they are in the best position to provide: the technical information on the traffic management measures that they apply. The public availability of this technical information creates the opportunity for the other parties in the model to step in and contribute to the formulation of the user-friendly information. It is expected that this will lead to multiple, complementary routes for the formulation of the user-friendly information. Thus, the user-friendly information emerges in ways driven by market players and stakeholders that would be difficult to design and lay down in advance in the transparency obligation.

### *5.2 Recent development: explicit rules on net neutrality in the Netherlands*

Recently, the Dutch parliament discussed and introduced a number of new rules for net neutrality in the new Dutch telecommunications law [13]. These new rules contain a number of explicit requirements on net neutrality that complement the transparency obligation addressed by the model proposed in this paper. The parliament has introduced these new rules because it felt that the transparency obligation and other rules from the universal service directive would not be sufficient to safeguard open access to services and applications on the Internet for end users.

For the most part, the new explicit requirements on net neutrality are implemented in new rules for ISPs. Some of the key elements of these new rules are:

- ISPs are not allowed to hinder or slow down applications and services on the Internet, except in certain specific situations.
- One of these specific situations is network congestion. ISPs are allowed to take measures that hinder or slow down applications to minimise the effects of congestion, as long as they treat equal types of traffic equally.
- Other specific situations in which ISPs are allowed to take such measures are related to spam prevention and reducing the effects and risks of botnets.
- ISPs are not allowed to make the tariffs of Internet access services dependent on the services and applications which are offered or used via these services.

The new rules clearly have impact on some of the subjects discussed in this paper. For example, the VoIP blocking use case from section 2.2 is no longer relevant in the Netherlands, as this type of traffic management is probably not allowed under the new rules. On the other hand, the transparency obligation will play an important role when it comes to other traffic management measures, such as those used by ISPs during congestion and for SPAM and botnet prevention. When evaluating whether the Internet access services offered by ISPs are in accordance with the new rules, the technical information from the transparency model plays a key role:

1. Which traffic stream is subject to a special treatment through traffic management measures?
2. Which measures are applied to this traffic stream?
3. When are these measures applied?

The combination of the answers to question 1 and 2 is important to determine whether the ISPs “treat equal types of traffic equally”. The answer to question 3 is needed to determine whether the measures are applied in situations that are allowed by the rules, e.g. during network congestion or prevention of SPAM. It is thus seen that the role and importance of the technical information becomes larger under the new rules. In addition to its use in the provision of *transparent information* to end users and other stakeholders, it may now also be needed in the actual *assessment* of ISP traffic management measures by the relevant government authorities.

# References


[1] Preserving Internet Freedom: Guiding Principles for the Industry, Michael K. Powell, February 8, 2004, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-243556A1.pdf

[2] Verizon-Google Legislative Framework Proposal, August 9, 2010, via http://googlepublicpolicy.blogspot.com/2010/08/joint-policy-proposal-for-open-internet.html

[3] 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, December 23, 2010

[4] Network neutrality Guidelines for Internet neutrality, Post- og teletilsynet, February 24, 2009, http://www.npt.no/ikbViewer/Content/109604/ Guidelines%20for%20network%20neutrality.pdf

[5] Internet and network neutrality: Proposals and policy directions, Arcep, September 2010, http://www.arcep.fr/uploads/tx_gspublication/net-neutralite-orientations-sept2010-eng.pdf

[6] Traffic Management and 'net neutrality', A Discussion Document, OFCOM, June 24, 2010, http://stakeholders.ofcom.org.uk/binaries/consultations/net-neutrality/summary/netneutrality.pdf

[7] Canadian Radio-television and Telecommunications Commission, Telecom Regulatory Policy CRTC 2009-657, October 21, 2009, http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm

[8] Directive 2009/140/EC (Framework Directive) of the European Parliament and of the Council, November 25, 2009

[9] Questionnaire for the public consultation on the open internet and net neutrality in Europe, European Commission, Information Society and Media Directorate-General, Electronic Communications Policy, June 30, 2010

[10] Digital Agenda: Commission underlines commitment to ensure open internet principles applied in practice, European Commission press release IP/11/486, April 19, 2011

[11] The open internet and net neutrality in Europe, European Commission communication COM(2011) 222 final, April 19, 2011

[12] Directive 2009/136/EC (Universal Service Directive) of the European Parliament and of the Council, November 25, 2009

[13] Wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen, Amendement van het lid Verhoeven c.s., Tweede Kamer der Staten-Generaal, vergaderjaar 2010-2011, 32 549, Nr 29 (in Dutch)

[14] Takahashi, A.; Hands, D.; Barriac, V.; , "Standardization activities in the ITU for a QoE assessment of IPTV," Communications Magazine, IEEE , vol.46, no.2, pp.78-84, February 2008 doi: 10.1109/MCOM.2008.4473087

[15] Vakali, A.; Pallis, G., "Content delivery networks: status and trends," Internet Computing, IEEE, vol.7, no.6, pp. 68- 74, Nov.-Dec. 2003, doi: 10.1109/MIC.2003.1250586

[16] Pathan, M., Buyya, R.,Vakali, A, Content Delivery Networks: State of the Art, Insights, and Imperatives, Lecture Notes in Electrical Engineering, Springer , 2008, Volume 9, Part I, 3-32

[17] AT&T Extends VOIP to 3G Network for iPhone, AT&T press release, October 6, 2009 at http://www.att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=27207

[18] Comcast Statement on FCC Internet Regulation Decision, August 1, 2008 at http://www.comcast.com/About/PressRelease/PressReleaseDetail.ashx?PRID=786

[19] Rogers Network Management Policy, August 11, 2011 at http://www.rogers.com/web/content/network_management

[20] Bell: Network management, August 11, 2011 at http://internet.bell.ca/index.cfm?language=en&method=content.view&content_id= 12119

[21] BEREC Response to the European Commission's consultation on the open Internet and net neutrality in Europe, BoR (10) 42, September 30, 2010

[22] Transparantie over netneutraliteit, TNO-rapport RA35383, December, 2, 2010 (in Dutch)

[23] M-lab | Measurement lab, http://www.measurementlab.net

[24] 3GPP TS 23.107, Quality of Service (QoS) concept and architecture, V9.1.0 (2010-06), via http://www.3gpp.org/ftp/Specs/html-info/23107.htm

[25] RFC2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, http://tools.ietf.org/html/rfc2474

[26] Regeling universele dienstverlening en eindgebruikersbelangen (in Dutch), at www.overheid.nl