TNO Informatie- en Communicatietechnologie

Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek / Netherlands Organisation for Applied Scientific Research

ONGERUBRICEERD

Brassersplein 2
Postbus 5050
2600 GB Delft

www.tno.nl

T +31 88 866 70 00
F +31 88 866 70 57
info-ict@tno.nl

TNO-rapport

RA35383

Transparantie over netneutraliteit

Datum	2 december 2010
Versie	1.0 (definitief)
Auteurs	Pieter Nooren, Mark Prins
Reviewers	Erik Fledderus, Pieter Venemans
Opdrachtgever	Ministerie van Economische Zaken, Landbouw & Innovatie
Projectnummer	035.33844
Aantal pagina's	51 (incl. bijlagen)
Aantal bijlagen	2

Samenvatting

Achtergrond

Netneutraliteit is al een aantal jaren een onderwerp van flinke discussie binnen de Internet community. In de kern gaat de netneutraliteitsdiscussie over de mate waarin verschillende soorten verkeer op het Internet verschillend mogen worden behandeld. In de nieuwe Europese kaderrichtlijn zijn beleidsdoelen rondom netneutraliteit opgenomen. Ter ondersteuning hiervan wordt onder meer een transparantieverplichting voor ISPs ingevoerd, opgenomen in de nieuwe universeledienstrichtlijn. Het doel van deze transparantieverplichting is eindgebruikers op een begrijpelijke manier inzicht te geven in de traffic management methoden die ISPs toepassen en welke gevolgen die voor hen hebben. Deze gevolgen kunnen liggen in de toegang tot diensten die de eindgebruikers hebben en de dienstkwaliteit die ze ervaren. De gebruiker kan deze informatie dan laten meewegen in zijn keuze tussen ISPs of besluiten over te stappen naar een andere ISP als hij vindt dat zijn ISP voor hem ongewenste traffic management methoden toepast. Op deze manier gaat van de transparantieverplichting een sturende werking uit op de ISPs.

Het Nederlandse Ministerie van Economische Zaken, Landbouw & Innovatie (EL&I) heeft de taak om de transparantieverplichting uit de Europese universeledienstrichtlijn verder in te vullen en te implementeren in Nederlandse wet- en regelgeving. EL&I heeft de hoofdlijnen van de transparantieverplichting al opgenomen in voorstellen voor de nieuwe Telecommunicatiewet[1]. EL&I voorziet dat de transparantieverplichting verder wordt uitgewerkt in lagere regelgeving. Het onderzoek beschreven in dit rapport richt zich op de inhoudelijke aspecten van deze verdere uitwerking.

Vraagstelling van EL&I aan TNO

De vraag van EL&I aan TNO valt uiteen in twee delen:

1. Wat zijn de uitgangspunten die moeten gelden voor transparantie? De uitgangspunten voor transparantie bepalen voor een belangrijk deel de uiteindelijke reikwijdte van de transparantieverplichting.
2. Welke variabelen moeten transparant worden? De vraag is hier welke inhoud en vorm van de informatie het beste bijdraagt aan het gewenste effect, namelijk de ISPs ertoe bewegen hun verkeer zodanig te managen dat het aan de wensen van eindgebruikers tegemoet komt.

EL&I wil de antwoorden op deze vragen gebruiken bij het opstellen van de (lagere) regelgeving die de transparantieverplichting inhoudelijk gaat vastleggen.

Aanpak

TNO heeft voor het beantwoorden van de twee bovenstaande vragen gebruik gemaakt van publieke bronnen en eigen expertise op het gebied van netwerktechnologieën, traffic management en hun relatie met (Internet) diensten. Daarnaast is gebruik gemaakt van de

[1] Zo bepaalt artikel 7.3 van het wetsvoorstel onder meer dat aanbieders van openbare elektronische communicatienetwerken en –diensten informatie bekendmaken over “eventuele beperkingen van de toegang tot of het gebruik van diensten en toepassingen” en over “de door de aanbieder ingestelde maatregelen bij congestie en de gevolgen daarvan voor de kwaliteit van de dienstverlening”.

bijdragen die ISPs, content providers, consumentenorganisaties en andere belanghebbenden hebben geleverd in twee workshops.

Bevindingen

1. Uitgangspunten en reikwijdte voor transparantie

Vanuit het wetsvoorstel Telecommunicatiewet moet een transparantieverplichting worden opgelegd aan aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten. In de praktijk zal een dergelijke verplichting gaan gelden voor ISPs. De reikwijdte van de verplichting wordt bepaald door een afbakening op vijf punten. In dit rapport wordt voorgesteld dat een transparantieverplichting aan de orde is:

1. Voor die traffic management maatregelen waarover de aanbieder *controle* of *zeggenschap* heeft.
   Hierbij kunnen traffic management maatregelen waarover de aanbieder *zeggenschap* heeft buiten de netwerken vallen waarover de aanbieder complete *controle* heeft.
2. Voor aanbieders van *vaste* netwerken en diensten en voor aanbieders van *mobiele* netwerken en diensten.
3. Voor aanbieders die zich richten op *particuliere* eindgebruikers en voor aanbieders die zich richten op *zakelijke* eindgebruikers.
   Een kanttekening hierbij is dat de praktische uitwerking van de transparantieverplichting in de grootzakelijke markt in een aantal situaties deels via de met eindgebruikers afgesloten SLAs kan lopen.
4. Voor traffic management maatregelen die aanbieders nemen in de *internettoegangsdienst* èn voor het effect dat de door hen geleverde *managed services* hebben op de internettoegangsdienst als geheel.
   Het opnemen van het effect van managed services op de internettoegangsdienst is een uitbreiding van de reikwijdte ten opzicht van traditionele analyses waarin alleen het effect van maatregelen toegepast op verkeerstromen binnen de internettoegangsdienst wordt meegenomen. Deze uitbreiding is van belang vanuit de verwachting dat managed services in de toekomst in aantal en belang zullen groeien en het effect dat de managed services kunnen hebben op de eveneens belangrijke internettoegangsdienst.
5. Binnen de internettoegangsdienst voor traffic management maatregelen die leiden tot het *verschillend behandelen van verkeerstromen.*

2. Transparant te maken informatie, betrokken partijen en processen

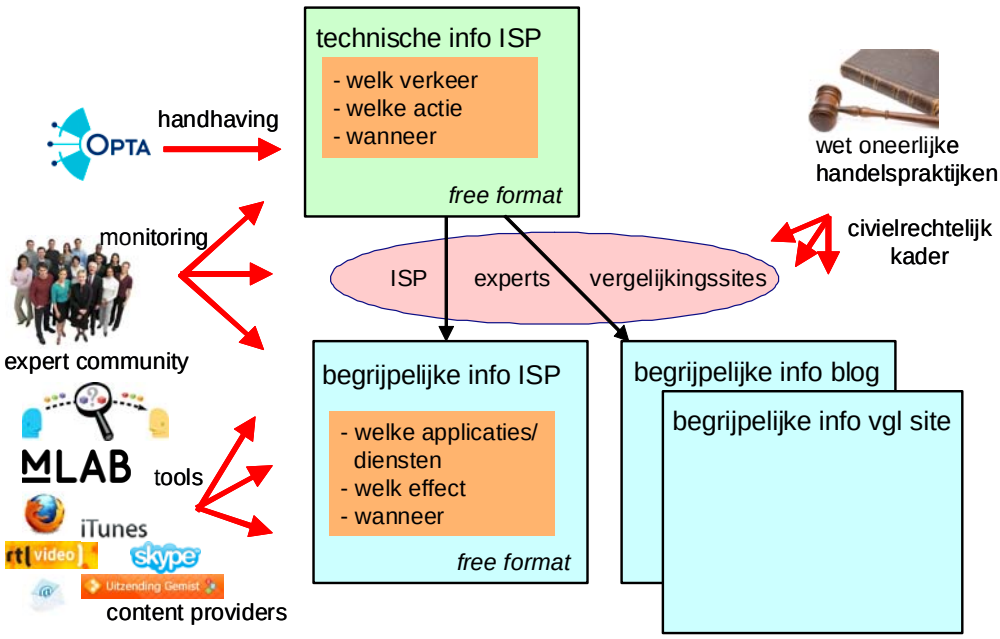
De informatie over traffic management maatregelen die vanuit de transparantieverplichting beschikbaar komt, moet leiden tot de gewenste sturende werking richting ISPs. Dit effect is het hoofddoel van de transparantieverplichting. Daarnaast moeten de informatie en de processen eromheen voldoen aan aantal bijkomende criteria zoals goede handhaafbaarheid, toekomstvastheid, vergelijkbaarheid, toegankelijkheid, beperkte kosten voor de betrokken marktpartijen, waarborgen voor netwerkintegriteit en correcte omgang met de concurrentiegevoeligheid van informatie. Dit laat zien dat de vorm en inhoud van de informatie in nauwe samenhang met de betrokken partijen en de processen waarin ze een rol spelen moet worden beschouwd.

In het voorgestelde transparantiemodel hebben niet alleen de ISPs, maar ook een reeks andere marktpartijen en belanghebbenden een rol, zoals OPTA als handhavende instantie, content providers, vergelijkingssites en experts uit de Internet community. De transparant te maken

informatie wordt daarom in nauwe samenhang behandeld met de inbreng van de diverse partijen bij het opstellen, interpreteren, vertalen en controleren van de transparante informatie. Het voorstel in dit onderzoek is om bij het inrichten van de transparantieverplichting onderscheid te maken tussen twee soorten informatie: technische en begrijpelijke informatie.

- De *technische informatie* beschrijft in technische termen de traffic management maatregelen die een ISP instelt. Deze informatie biedt met name voor experts een duidelijke toegang tot de feitelijke technische maatregelen. Hierbij gaat het om de antwoorden op drie vragen:
  – Welke verkeerstroom wordt door traffic management maatregelen speciaal behandeld?
  – Welke maatregel wordt toegepast op deze verkeerstroom?
  – Wanneer wordt deze maatregel toegepast?

  ISPs zijn in verreweg de beste positie om technische informatie te verschaffen over de traffic management maatregelen die zij nemen. Gezien het belang van de technische informatie voor de handhaving èn voor het opstellen van begrijpelijke informatie, is het voorstel om ISPs te verplichten de technische informatie te verschaffen over hun traffic management maatregelen, voor zover ze binnen de hierboven beschreven reikwijdte vallen. Te verwachten is dat OPTA een rol krijgt in de handhaving van de verplichting. De mate van detail in de informatie die de ISPs moeten opleveren is bepaald door een afweging van de eerder genoemde criteria. In dit rapport wordt een uitgebreide analyse gemaakt van de vereiste mate van detail, mede op basis van de bijdragen van de deelnemers in de workshops. Daaruit volgt bijvoorbeeld dat de technische omschrijving van het “welke verkeerstroom” deel van de technische informatie tenminste moet ingaan op de (klassen van) toepassingen inclusief de opsomming van de (combinaties van) technische parameters die het verkeer karakteriseren.



- De *begrijpelijke informatie* beschrijft de gevolgen van de traffic management maatregelen voor de eindgebruikers, in termen die een brede groep eindgebruikers begrijpt. Hierbij gaat het om:

- Welke applicaties en diensten een speciale behandeling krijgen.
- Wat het effect van de speciale behandeling is of kan zijn op de beleving van de dienst door de eindgebruiker.
- Wanneer dit effect merkbaar is.

De voor de gemiddelde eindgebruiker begrijpelijke informatie ontstaat door vertaling van de technische informatie naar de belevingswereld van de eindgebruiker. Op hoofdlijnen is deze vertaling relatief eenvoudig. Tegelijkertijd is de vertaling deels subjectief, onder meer doordat er naast de traffic management maatregelen andere factoren van invloed zijn op de dienstbeleving van de eindgebruiker.

In dit onderzoek wordt voorgesteld om geen verplichting in te voeren voor het beschikbaar maken van begrijpelijke informatie. De verwachting is dat ISPs uit zichzelf al een vertaling naar begrijpelijke informatie zullen maken om de technische informatie, die ze wel verplicht op een goed zichtbare plaats moeten publiceren, aan hun (potentiële) klanten toe te lichten. Daarnaast is het in veel gevallen lastig om een eenduidige verplichting te formuleren voor de deels subjectieve vertaalslag van technische naar begrijpelijke informatie.

Als de gevraagde technische informatie beschikbaar is, zijn naast de ISPs ook andere partijen in staat om de vertaling te maken van technische naar voor de eindgebruikers begrijpelijke informatie. Dat zijn bijvoorbeeld technische experts uit de Internet community, vergelijkingssites en content providers. De begrijpelijke informatie ontstaat via deze routes op een door marktpartijen en belanghebbenden gestuurde manier. Verschillende vergelijkingssites, fora en bloggers zullen zich voor wat betreft de inhoud en de presentatie van hun begrijpelijke informatie richten op de aspecten die voor hun doelgroep het meest relevant zijn. Partijen die zich benadeeld voelen door gepubliceerde informatie kunnen een beroep doen op de bestaande civielrechtelijke middelen zoals de Wet Oneerlijke Handelspraktijken.

Summary

Background

Net neutrality has, for a number of years, been a topic of often heated discussion in the Internet community. The crux of the issue is the extent to which different types of traffic on the Internet may be treated differently. 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. 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. For example, the traffic management methods can have consequences for the access that end users have to services and in the service quality that they experience. Based on the information on traffic management that is provided to them, end users can make an informed decision 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.

The Dutch Ministry for Economic Affairs, Agriculture and Innovation has the responsibility to implement the transparency obligation from the universal service directive in Dutch legislation. The main elements of the obligation have already been incorporated in the proposal for the new Telecommunications law. The ministry expects to implement the obligation in more detail in additional regulations. The analysis in this report focuses on this more detailed implementation.

Questions from the Ministry to TNO

The question from the Ministry to TNO has two components:
1. What are the basic principles for the transparency? These principles determine to a large extent the scope that the transparency obligation will have.
2. Which parameters should be made transparent? The question here is which information and form best contribute to the desired effect of the transparency, that is to influence the way ISPs apply traffic management in such a way that it answers the needs and wishes of the end users.

The Ministry plans to use the answers to these questions in their implementation of the transparency obligation in Dutch telecommunication regulations.

Approach

TNO has answered the two questions above based on a number of public sources and its own expertise in network technologies, traffic management and their relation with (Internet) services. TNO has also used the contributions that ISPs, content providers, consumer interest groups and other stakeholders have made in two workshops.

Findings

1. Basic principles and scope for transparency

The proposal for the new Telecommunications law stipulates that a transparency obligation must apply to providers of public electronic communication networks or services. In practice, the obligation will apply to ISPs. The scope of the obligation is determined by a demarcation on five points. In this report, it is proposed that a transparency obligation is appropriate:

1. For traffic management measures over which the provider has *control* or *significant influence.*
   Here, traffic management measures over which the provider has a *significant influence* can occur outside the networks over which the provider has full *control*.
2. For providers of *fixed* networks and services and for providers of *mobile* networks and services.
3. For providers of services to *consumers* and for providers of services to *business users.*
   It should be noted that in the market for large business customers, the practical implementation of the transparency obligation may be partly based on the Service Level Agreements (SLAs) between the providers and the business customers.
4. For traffic management measures that providers take in the *Internet access service* and for the effect that the *managed services* that they provide have on the Internet access service as a whole.
   The inclusion of the effect of managed services on the Internet access service is an extension of the scope compared to traditional analyses in which only the effect of measures on traffic streams within the Internet access service is considered. This extension is important, as it is expected that managed services will grow both in number and in importance in the future and the effect that managed services can have on the important Internet access service will also increase.
5. Within the Internet access service, for traffic management measures that lead to a *different treatment of traffic streams.*

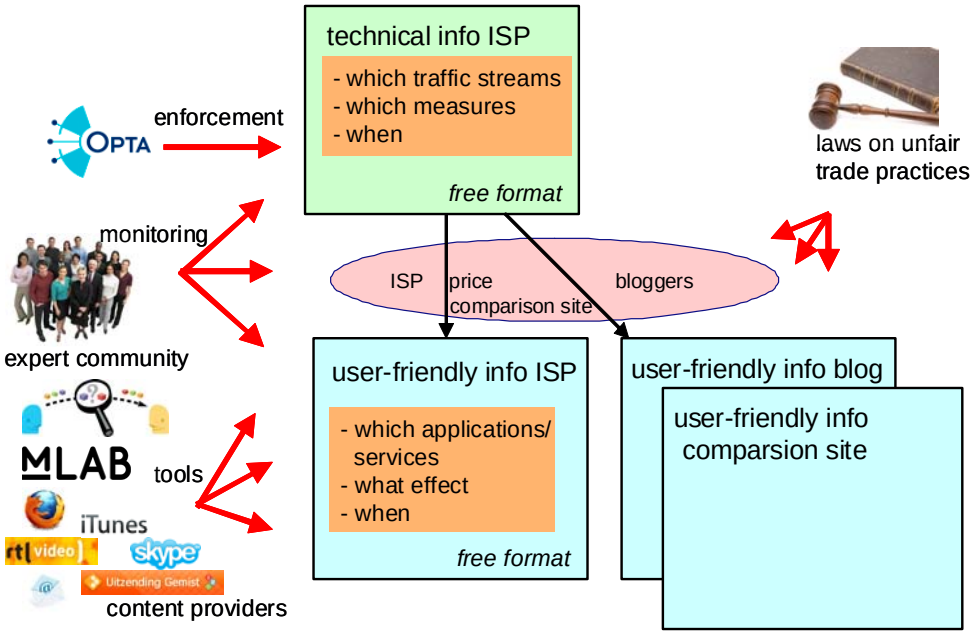
2. Transparent information, parties and processes involved

The information on traffic management measures that becomes available through the transparency obligation should lead to the desired influencing of the ISPs. This effect is the main objective of the transparency obligation. Apart from this, the information and related processes must meet a number of other criteria. For example, the regulator should be able to monitor and enforce the implementation of the obligation. Furthermore, the information and processes should be future proof, comparable, accessible, bring limited additional costs for the parties involved, maintain network integrity and ensure a proper treatment of the potential commercial sensitivity of the information. This shows that the content and form of the information should be considered in close connection to the parties involved and the process in which they play a role.

The transparency model proposed in this report includes roles for the ISPs, but also for a range of other market players and stakeholders, such as the Dutch regulator OPTA, content providers, price comparison sites and experts from the Internet community. The transparency information is therefore considered together with the contributions that the various parties bring in the formulation, interpretation, translation and checking of the information. The proposal in this report is to distinguish between two types of information in the implementation of the transparency obligation: 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 answers to three questions are relevant here:
  - Which traffic stream is subject to a special treatment through traffic management measures?
  - Which measures are applied to this traffic stream?
  - When are these measures applied?

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 for enforcement and for the formulation of user-friendly information, it is proposed here to oblige the ISPs to provide the technical information on the traffic management measures they apply, to the extent that they are within the scope defined above. It is foreseen that the regulator OPTA will have a role in the enforcement of the obligation. The level of detail in the information that the ISPs should provide is determined by weighing the criteria mentioned earlier. This report provides a detailed analysis of the required level of detail, partly based on the contributions that the workshop participants have made. Among other things, the analysis leads to the conclusion that the answer to the "which traffic stream" question should describe at least the (classes of) applications including a list of (combinations) of technical parameters that characterise the traffic.



- 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. Here, the answers to the following questions are relevant:
  - Which applications and services receive special treatment from traffic management?
  - What is the effect of the traffic management measures on the services as they are experienced by end users?
  - When is this effect noticeable?

  The user-friendly information is understandable for the average end user. It is derived by translating the technical information into its effect on the end user experience. To a large extent, this translation is relatively straightforward. At the same time, the translation is

partly subjective as there are also factors other than traffic management measures that affect the end user experience.

In this report, no obligation is proposed for the provision of user-friendly information. 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 this, it is in many cases difficult to formulate an unambiguous obligation for the partly subjective translation from technical to user-friendly information.

When the technical information is available, also other parties than the ISPs are able to translate the technical information to user-friendly information understandable by a wider audience. These parties could be technical experts from the Internet community, price comparison sites and content providers. Through these alternative routes, the user-friendly information thus emerges in ways driven by market players and stakeholders. Different comparison sites, fora and blogs will tailor the content and presentation of their information to the audience they are targeting. Parties who feel that information published by others is damaging can seek to correct this through the existing laws on unfair trade practices.

Inhoudsopgave

Samenvatting **3**

Summary **7**

1 Inleiding **13**
1.1 Achtergrond: transparantie ter bevordering van netwerkneutraliteit 13
1.2 Vraag van EL&I aan TNO 14
1.3 Gebruikte bronnen 15
1.4 Afbakening 15
1.5 Leeswijzer 15

2 Uitgangspunten en reikwijdte voor transparantie **17**
2.1 Drie use cases ter illustratie 17
2.2 Dimensie 1: Domein waar ISP controle of zeggenschap over heeft 19
2.3 Dimensie 2: Vaste en mobiele internetdiensten 20
2.4 Dimensie 3: Particuliere en zakelijke eindgebruikers 21
2.5 Dimensie 4: Effect van managed diensten op internettoegangsdienst 22
2.6 Dimensie 5: Onderscheid tussen verkeerstromen binnen de internettoegangsdienst 24

3 Transparante informatie, betrokken partijen en processen **27**
3.1 Eisen aan model 27
3.2 Model op hoofdlijnen 28
3.3 Technische informatie: verplichting voor ISPs 31
3.4 Begrijpelijke informatie 37

4 Conclusie **41**
4.1 Uitgangspunten en reikwijdte voor transparantie 41
4.2 Transparant te maken informatie, betrokken partijen en processen 41

5 Referenties **45**

Bijlage(n)
A Passages uit relevante wet- en regelgeving
B Deelnemers aan workshops

1 Inleiding

1.1 Achtergrond: transparantie ter bevordering van netwerkneutraliteit

Netwerkneutraliteit, of kortweg netneutraliteit, is al een aantal jaren een onderwerp van flinke discussie binnen de Internet community. In de kern gaat de netneutraliteitsdiscussie over de mate waarin verschillende soorten verkeer op het Internet verschillend mogen worden behandeld. Technisch gezien kan dit “verschillend behandelen” worden bereikt met zogenaamd traffic management. Traffic management is een bekende en noodzakelijke functie in telecom netwerken, en ook in het Internet. Traffic management zorgt ervoor dat de beschikbare capaciteit in verbindingen en apparatuur op een goede manier kan worden gedeeld door de vele verkeersstromen die door een netwerk gaan. De netneutraliteitsdiscussie begint als in het traffic management onderscheid gemaakt wordt tussen verschillende verkeersstromen, bijvoorbeeld op basis van de bestemming van het verkeer of de soort applicatie waaraan het verkeer gerelateerd is. De analyse in dit rapport richt zich vooral op dit deel van de discussie.

In de VS heeft regelgever FCC al in 2004 voor het eerst standpunten over netneutraliteit ingenomen [1]. De discussie daar is recent weer flink opgelopen, o.a. naar aanleiding van een gezamenlijk voorstel van Google en Verizon [2]. Inmiddels hebben ook regelgevers en toezichthouders in verschillende andere landen consultaties uitgevoerd en uitspraken gedaan over netneutraliteit ([3], [4], [5], [6]).

Ook op Europees niveau is een aantal stappen gezet op het gebied van netneutraliteit. In de nieuwe Europese kaderrichtlijn zijn beleidsdoelen rondom netneutraliteit opgenomen [7]. Ter ondersteuning hiervan wordt onder meer een transparantieverplichting voor ISPs ingevoerd, die is opgenomen in de nieuwe universeledienstrichtlijn [8]. Het doel van deze transparantieverplichting is om eindgebruikers op een begrijpelijke manier inzicht te geven in de traffic management methoden die ISPs toepassen. De gebruiker kan deze informatie dan laten meewegen in zijn keuze tussen ISPs of besluiten over te stappen naar een andere ISP als hij vindt dat zijn ISP tekort schiet op het gebied van netneutraliteit. Op deze manier gaat van de transparantieverplichting een sturende werking uit op de ISPs: ISPs zullen bij hun overwegingen ten aanzien van traffic management functies hun eigen belangen en die van de consumenten zorgvuldig wegen. Immers, “slecht gedrag” op het gebied van netneutraliteit wordt zichtbaar gemaakt en vervolgens mogelijk “afgestraft” door vertrekkende klanten. Een aantrekkelijke eigenschap van dit transparantiemechanisme is dat het niet vraagt om lastig te vellen waardeoordelen over het al dan niet wenselijk, nodig en verantwoord zijn van traffic management technieken. Dit waardeoordeel wordt in feite overgelaten aan de eindgebruikers die hun mening laten weten door “met hun voeten te stemmen”. De recente consultatie van de Europese commissie over open Internet en netneutraliteit in Europa [9] gaat ook in op het transparantiemechanisme en het gewenste effect ervan.

Het Nederlandse Ministerie van Economische Zaken, Landbouw & Innovatie (EL&I) heeft de taak om de transparantieverplichting uit de Europese universeledienstrichtlijn verder in te vullen en te implementeren in Nederlandse wet- en regelgeving. EL&I heeft de hoofdlijnen van de transparantieverplichting al opgenomen in voorstellen voor de nieuwe Telecommunicatiewet ([10], [11], zie ook bijlage A). EL&I voorziet dat de transparantieverplichting nader wordt uitgewerkt in nieuwe versies van het Besluit Universele Dienstverlening en Eindgebruikersbelangen (BUDE) en de Regeling Universele

Dienstverlening en Eindgebruikersbelangen (RUDE). Het onderzoek beschreven in dit rapport richt zich op de inhoudelijke aspecten van deze nadere uitwerking.

In Nederland is al eerder nagedacht over het mechanisme om via transparantie te komen tot een sturende werking richting ISPs, onder meer in het kader van een studie uitgevoerd door Dialogic [12]. Daarin bleek onder meer dat de informatievoorziening door Nederlandse ISPs over hun traffic management maatregelen duidelijk nog te verbeteren viel. Dialogic stelt in haar rapport een aantal uitgangspunten voor die de gewenste reikwijdte van de transparantie afbakenen. Daarnaast wijst het rapport op de beperkingen van twee soorten informatie over traffic management maatregelen: feitelijke (technische) informatie en voor consumenten begrijpelijke informatie.

Een experimentele economische studie door TILEC [13] maakt aannemelijk dat meer informatie over de kwaliteit van breedband inderdaad leidt tot andere keuzes bij eindgebruikers en gedragsveranderingen bij aanbieders van breedband. Onder het koepelbegrip “kwaliteit van breedband” zouden ook de effecten van traffic management maatregelen gerekend kunnen worden. Een andere relevante conclusie van de studie is dat ook “onvolledige” transparantie tot andere keuzes en gedragingen leidt. Een belangrijk voorbeeld van “onvolledige” transparantie is de situatie waarin de eindgebruikers slechts over een deel van de informatie over de kwaliteit van breedband producten kunnen beschikken. Een andere relevante situatie met “onvolledige” transparantie doet zich voor als één deel van de eindgebruikers volledige informatie heeft en een ander deel van de eindgebruikers geen informatie. Deze conclusies over het effect van “onvolledige” transparantie zijn van belang in de analyse die in dit rapport wordt gemaakt over de typen informatie die transparant moeten worden gemaakt en de wijze waarop ze aan eindgebruikers worden aangeboden.

1.2 Vraag van EL&I aan TNO

De vraag van EL&I aan TNO valt uiteen in twee delen:
1. Wat zijn de uitgangspunten die moeten gelden voor transparantie?
2. Welke variabelen moeten transparant worden?

De antwoorden op deze vragen gaat EL&I gebruiken bij het opstellen van (lagere) regelgeving waarin de transparantieverplichtingen voor marktpartijen, in het bijzonder voor ISPs, worden vastgelegd.

Ad 1) De uitgangspunten voor transparantie bepalen voor een belangrijk deel de uiteindelijke reikwijdte van de transparantieverplichting. Hierbij gaat het om subvragen als: moet transparantie verschaft worden aan zowel particuliere als zakelijke gebruikers? Gaat het over zowel vaste als mobiele diensten? Over welke onderdelen in de totale internetketen strekt de transparantieverplichting zich uit?

Ad 2) Transparantie over traffic management maatregelen in de context van netneutraliteit betekent dat ISPs informatie aan het publiek beschikbaar stellen over de technische maatregelen die ze in hun netwerken nemen om verschillende verkeerstromen op verschillende manieren te behandelen. Voor de inhoud, vorm en uitgebreidheid van deze informatie zijn vele mogelijkheden denkbaar. De hoofdvraag is hier: Welke inhoud en vorm van de informatie draagt het beste bij aan het gewenste effect, namelijk een sturende werking richting ISPs, terwijl hij tegelijkertijd voldoet aan een aantal bijkomende criteria zoals goede handhaafbaarheid, toekomstvastheid en beperkte kosten voor de betrokken marktpartijen?

1.3 Gebruikte bronnen

TNO heeft voor het beantwoorden van de twee bovenstaande vragen gebruik gemaakt van publieke bronnen, eigen expertise en de bijdragen die marktpartijen en andere belanghebbenden hebben geleverd in twee workshops.

- Het startpunt voor de analyse van de uitgangspunten voor transparantie was het eerder genoemde Dialogic rapport. TNO heeft de analyse van Dialogic voortgezet en op punten aangepast, op basis van recente Europese richtlijnen, Nederlandse wetsvoorstellen en een aantal nieuwe ontwikkelingen in de markt.
- Bij het formuleren van het voorstel voor de vorm en inhoud van de transparant te maken informatie heeft TNO in eerste instantie gebruik gemaakt van zijn eigen expertise over de Nederlandse vaste en mobiele netwerkarchitecturen, de traffic management mechanismen die daarin worden toegepast en de wijze waarop deze mechanismen doorwerken in verschillende diensten.
- Zowel de uitgangspunten voor transparantie als het voorstel voor de vorm en inhoud van de informatie zijn uitgebreid met belanghebbenden besproken en doorgenomen in twee interactieve workshops. Onder de deelnemers aan de workshops waren vaste en mobiele ISPs, consumentenorganisaties en content providers. Bijlage B geeft een compleet overzicht van de deelnemers. TNO heeft de inzichten opgedaan tijdens de workshops gebruikt om tot keuzes te komen tussen verschillende mogelijke opties en zijn voorstellen aan te scherpen.

1.4 Afbakening

Bij het lezen van dit rapport en het hanteren van de conclusies is de volgende afbakening van belang:

- Het rapport beperkt zich tot het verschaffen van transparantie over traffic management maatregelen door ISPs. Het gaat niet in op de vraag of de traffic management maatregelen zelf al dan niet nuttig, gepast of gewenst zijn. Het beschrijven van use cases waarmee bepaalde traffic management methoden worden geïllustreerd betekent dan ook niet dat de auteurs van dit rapport deze use cases wenselijk of juist onwenselijk vinden.
- Het in hoofdstuk 3 voorgestelde model is ontwikkeld om EL&I te ondersteunen bij het formuleren van regelgeving rondom transparantie. TNO ziet het model als een nuttig middel voor het afwegen van verschillende mogelijkheden om transparantie te verschaffen. Voor de betrokken marktpartijen is vooral de uiteindelijke regelgeving van belang. Deze regelgeving wordt door EL&I opgesteld op basis van haar eigen afwegingen en gebruik makend van diverse bronnen, waaronder dit rapport.
- Dit rapport gaat niet in op de vraagstelling in de Tweede Kamer motie Aasted Madsen-van Stiphout-Vos [14] die “verzoekt de regering te bewerkstelligen dat providers voorafgaand aan het afsluiten of verlengen van internetabonnementen op voor leken transparante wijze informatie geven over de realistisch te bereiken snelheden van vaste en mobiele internetabonnementen”. De analyse in dit rapport raakt op een aantal plaatsen wel de vraag uit deze motie. Dit wordt in het rapport duidelijk aangegeven. Het rapport gaat ook niet in op mogelijke “minimumvoorschriften inzake de kwaliteit van openbare elektronische communicatiediensten” genoemd in artikel 7.4a van het wetsvoorstel Telecommunicatiewet.

1.5 Leeswijzer

De opbouw van dit rapport volgt de vraagstelling van EL&I. Na deze inleiding volgt in hoofdstuk 2 de analyse van de uitgangspunten voor transparantie. Dit leidt tot de gezochte

afbakening van de verplichting. Daarna gaat hoofdstuk 3 in op de inhoud van de op te leveren informatie en de mate van detail daarin. Hierbij komen ook de marktpartijen en stakeholders die een rol spelen bij het opstellen, interpreteren, vertalen en controleren van de informatie uitgebreid aan de orde. Het rapport sluit af met het formuleren van de belangrijkste conclusies in hoofdstuk 4.

2 Uitgangspunten en reikwijdte voor transparantie

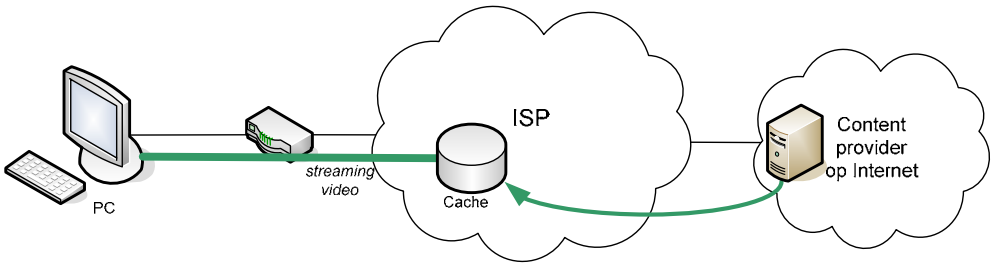
Dit hoofdstuk gaat in op de uitgangspunten voor transparantie die voor een belangrijk deel de uiteindelijke reikwijdte van de transparantieverplichting bepalen. Hierbij gaat het om subvragen als: moet transparantie verschaft worden aan zowel particuliere als zakelijke gebruikers? Gaat het over zowel vaste als mobiele diensten? Over welke onderdelen in de totale internetketen strekt de transparantieverplichting zich uit? Voor een deel zijn de uitgangspunten en reikwijdte van de transparantieverplichting al vastgelegd in de Europese richtlijnen en de voorstellen voor vertaling daarvan in de Nederlandse Telecommunicatiewet. Bijlage A bevat een aantal relevante passages uit deze wet- en regelgeving. Voor het vastleggen van de transparantieverplichting in lagere regelgeving is een verdere detaillering van de uitgangspunten en reikwijdte nodig. De volgende paragrafen beschrijven deze detaillering aan de hand van een analyse van vijf dimensies waarin een afbakening van de transparantieverplichting nodig is, waaronder de hierboven genoemde dimensies vast-mobiel en particulier-zakelijk. Het resultaat hiervan is een afbakening van de reikwijdte van de transparantieverplichting op ieder van die vijf dimensies. De vijf dimensies zijn eerder al kort geanalyseerd door Dialogic [12]. De uitgebreidere analyse in het huidige onderzoek is met de deelnemers aan de workshops doorgenomen. De reacties van de deelnemers zijn gebruikt om de analyse te toetsen en de reikwijdte van de transparantieverplichting zo duidelijk mogelijk af te bakenen.

2.1 Drie use cases ter illustratie

Om de analyse van de uitgangspunten en reikwijdte concreter te maken worden hier drie use cases geïntroduceerd waarin transparantie over netwerkneutraliteit aan de orde is. Later in dit rapport worden deze use cases ook gebruikt voor het geven van voorbeelden bij de inhoudelijke invulling van de transparantieverplichting.

2.1.1 Use case 1: Efficiënter afleveren streaming video

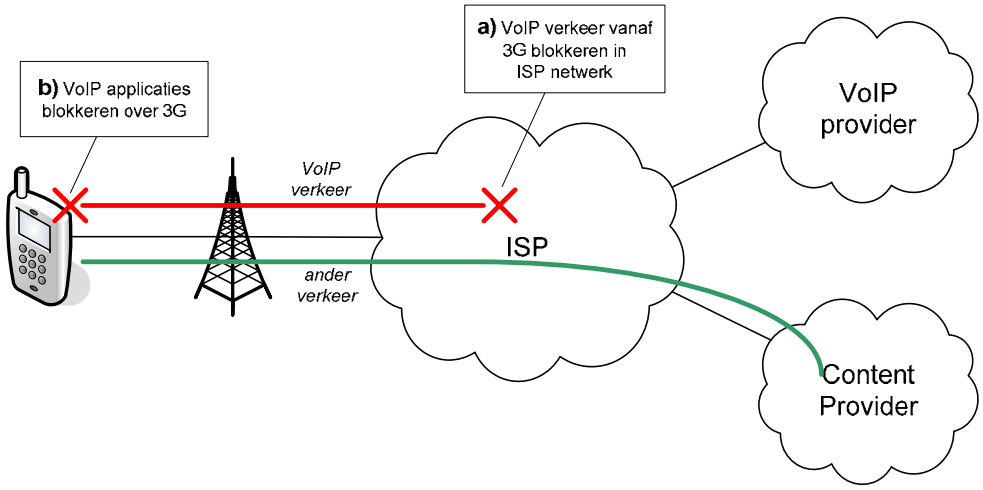
Bij streaming video bekijkt een gebruiker videomateriaal dat op zijn verzoek naar hem wordt verzonden (“*gestreamd*”) vanaf een server. Bekende voorbeelden van websites waarop gebruikers streaming video’s kunnen aanvragen zijn YouTube [15] en Uitzending Gemist [16]. Streaming video verkeer is gevoelig voor vertragingen en andere ongewenste effecten in het netwerk. Daarnaast legt het beslag op een groeiend deel van de bandbreedte in ISP netwerken. Een aanpak die zowel de kwaliteit van streaming video kan verbeteren als het beslag op bandbreedte kan verminderen is het inzetten van caches in het ISP netwerk, waarin populaire content dichter bij de klanten wordt opgeslagen. Caching is een belangrijke technische component van zogenaamde Content Delivery Networks (CDNs). Voor eindgebruikers betekent dit dat ze bepaalde populaire video’s, namelijk die in de cache/CDN, in een aantal gevallen met hogere kwaliteit kunnen zien dan andere video’s.



Figuur 1. Use case: efficiënter afleveren streaming video.

2.1.2 *Use case 2: VoIP verkeer op mobiele netwerken blokkeren*

Uit de afgelopen jaren is een aantal gevallen bekend waarin gebruikers geen VoIP applicaties konden gebruiken binnen hun mobiele data dienst. In een aantal gevallen ([17], [18]) was sprake van (plannen voor) het herkennen en blokkeren van VoIP verkeer in het ISP netwerk, zie optie a) in Figuur 2. Een ander bekend geval is het gebruik van Skype op een iPhone over mobiele netwerken. In eerste instantie was het met de Skype app beschikbaar voor de iPhone wel mogelijk om over Wireless LAN netwerken VoIP gesprekken te voeren, maar niet over mobiele netwerken (zie optie b) in Figuur 2). Inmiddels is via de Apple app store een versie van Skype beschikbaar gekomen die wel over mobiele netwerken werkt [19].

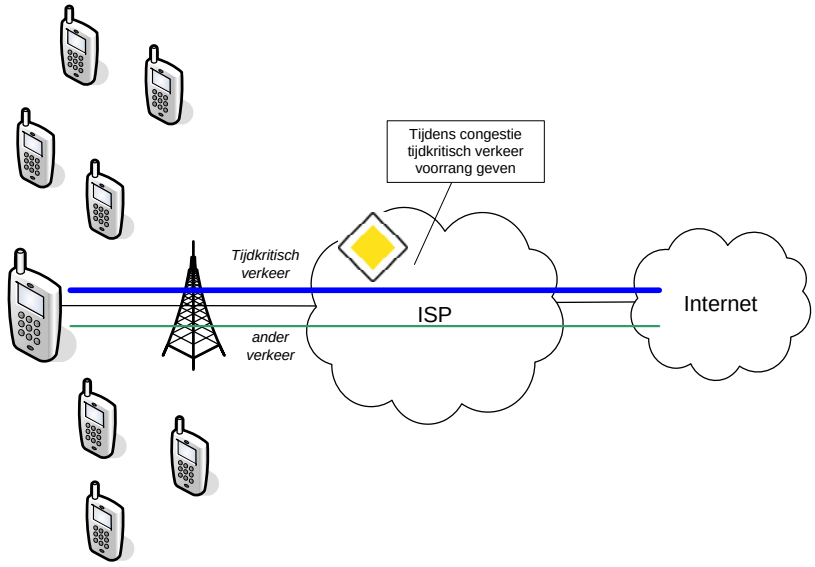


Figuur 2. Use case: blokkeren van VoIP volgens twee methoden: a) blokkeren in het netwerk en b) blokkeren via de applicatie op de mobiele terminal.

2.1.3 *Use case 3: Tijdkritische applicaties voorrang geven bij congestie*

Figuur 3 schetst een maatregel die mobiele operators mogelijk kunnen nemen bij congestie in het radionetwerk. Mobiele operators houden bij de planning en dimensionering van hun netwerken rekening met diverse scenario's waarin lokaal of over het hele netwerk een plotseling sterk stijgende vraag naar capaciteit ontstaat. Om bedrijfseconomische redenen kan niet voldoende capaciteit worden aangelegd om in alle scenario's aan de vraag te voldoen. In de hier geschetste use case worden in gevallen waarin de capaciteit tekort schiet de gevolgen voor de dienstbeleving van de gebruikers verzacht. Dat gebeurt door diensten die tijdkritisch zijn en daardoor de meeste last van congestie hebben, voorrang te geven boven diensten die minder tijdkritisch zijn. Bij tijdkritische diensten valt bijvoorbeeld te denken aan VoIP,

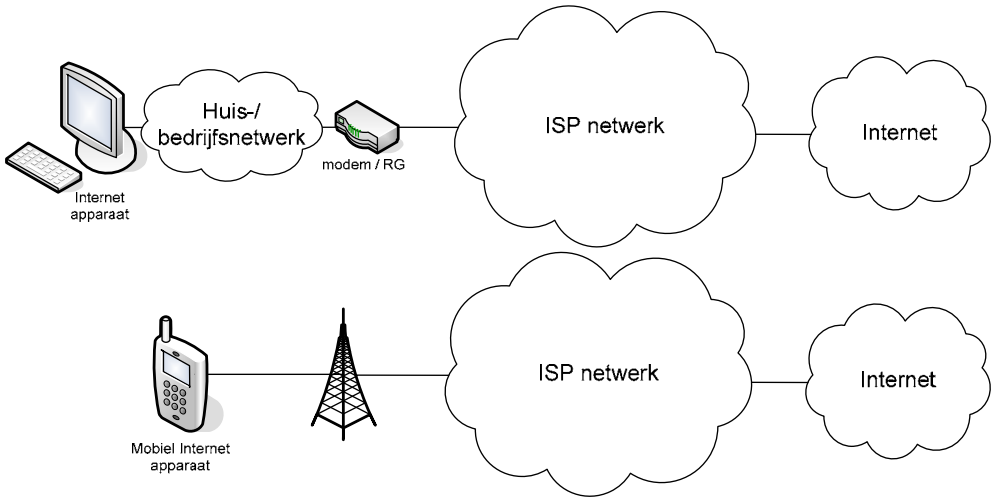
videoconferencing en webbrowsing. E-mail is een typisch voorbeeld van een niet-tijdkritische dienst.



Figuur 3. Use case: tijdkritische applicaties voorrang geven bij congestie.

2.2 Dimensie 1: Domein waar ISP controle of zeggenschap over heeft

Bij het leveren en afnemen van Internet diensten is in het algemeen een aaneenschakeling van netwerken betrokken, zie Figuur 4. Verschillende netwerken in de keten kunnen door verschillende aanbieders worden geleverd. In elk netwerk kunnen traffic management maatregelen worden toegepast die ervoor zorgen dat verschillende soorten verkeer verschillend worden behandeld.



Figuur 4. De aaneenschakeling van netwerken in de breedband Internet keten in typische vaste netwerken (boven) en mobiele netwerken (onder).

Artikel 7.3 van het wetsvoorstel Telecommunicatiewet spreekt van “aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten”

waarvoor de transparantieverplichting kan gelden. Uit de universele dienstrichtlijn blijkt verder dat de transparantie verschaft moet worden aan eindgebruikers van de diensten. In de praktijk betekent dit dat de transparantieverplichting gaat gelden voor ISPs, aangezien zij de internettoegangsdiensten aan eindgebruikers leveren. Het ligt voor de hand om de transparantieverplichting voor ISPs te beperken tot de delen van het netwerk waarover ISPs controle dan wel zeggenschap hebben, en daarmee invloed op de traffic management maarregelen.

- Over de traffic management maatregelen in hun eigen netwerk hebben ISPs volledige controle. Deze controle strekt zicht uit van het afleverpunt bij de eindgebruiker, bijvoorbeeld op een modem of mobiele terminal, aan de ene kant tot de verbindingen met de IP netwerken in het publieke Internet aan de andere kant. Op dit deel van de keten is de in het volgende hoofdstuk nader uitgewerkte transparantieverplichting aan de orde. Voor de bouw van een eigen netwerk maken ISPs in verschillende gevallen gebruik van (wholesale) netwerk- en dienstcomponenten geleverd door andere aanbieders. Dergelijke ingekochte wholesale componenten worden in de hier gemaakte analyse gerekend tot het eigen netwerk van de ISP.
- Over de IP netwerken die samen het publieke Internet vormen, en de servers en platformen die daaraan gekoppeld zijn heeft de ISP in het algemeen geen controle of zeggenschap. Een transparantieverplichting is daarom voor deze onderdelen van de keten niet aan de orde. De IP netwerken in het publieke Internet kunnen afhankelijk van de dienst en precieze netwerkbelasting wel een grote invloed hebben op de dienstkwaliteit die de eindgebruiker ervaart.
- Het beheer van het huisnetwerk (of bedrijfsnetwerk) is in eerste instantie een zaak voor de eindgebruiker en valt niet onder de controle van de ISP. Toch kan hier wel degelijk sprake zijn van zeggenschap en daarmee invloed van de ISP over traffic management maatregelen. Hiervan is sprake als de ISP bepaalde apparatuur (zoals modems of terminals) aanbiedt of voorschrijft die door de leverancier van de apparatuur worden geleverd met bepaalde traffic management maatregelen. In de universeledienstrichtlijn staan in dit verband bepalingen over "*beperkingen die de leverancier heeft opgelegd met betrekking tot het gebruik van geleverde eindapparatuur"* (artikel 20(1)(b)). Deze verplichting komt ook terug in artikel 7.1 en de toelichting daarop in het wetsvoorstel voor de Nederlandse telecommunicatiewet. Deze invloed van de ISP speelt in de use case "VoIP verkeer op mobiele netwerken blokkeren" uit sectie 2.1.2. In een variant b) van deze use case kiest de ISP ervoor om in combinatie met bepaalde abonnementen een mobiele terminal te leveren waarop de leverancier van de terminal geen VoIP verkeer over mobiele netwerken ondersteunt. Via de keuze voor de geleverde terminal heeft de ISP invloed op de traffic management maatregelen. Ook hier is daarom een transparantieverplichting aan de orde.

Dimensie 1: Een transparantieverplichting voor aanbieders van netwerken en diensten is aan de orde voor de traffic managementmaatregelen waarover de aanbieder controle of zeggenschap heeft.

2.3 Dimensie 2: Vaste en mobiele internetdiensten

Uit de praktijk blijkt dat in zowel vaste als mobiele netwerken door ISPs in een aantal situaties traffic management maatregelen zijn ingesteld die voor gebruikers de toegang tot diensten op het Internet beperken. Bij vaste netwerken gaat het daarbij bijvoorbeeld om het beperken van peer-to-peer (P2P) filesharing verkeer. P2P filesharing wordt onder meer gebruikt voor het uitwisselen van muziek- en videobestanden. Van het beperken van P2P verkeer zijn verschillende voorbeelden bekend uit het buitenland ([20], [21], [22], [23]). Ook

in Nederland is ten minste één geval bekend. Bij mobiele netwerken gaat het bijvoorbeeld over het blokkeren van VoIP verkeer, volgens de methoden geschetst in de use case in paragraaf 2.1.2. Deze praktijkvoorbeelden laten zien dat een transparantieverplichting zowel voor vaste als mobiele netwerken aan de orde is.

Zoals al aangehaald in de vorige paragraaf spreekt artikel 7.3 van het wetsvoorstel Telecommunicatiewet van “aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten”. Het artikel maakt hierin geen onderscheid tussen aanbieders van vaste of mobiele diensten.

Dimensie 2: Een transparantieverplichting is aan de orde voor aanbieders van vaste netwerken en diensten en voor aanbieders van mobiele netwerken en diensten.

Voor eindgebruikers is het daarbij wenselijk dat de manier waarop transparantie wordt verschaft over traffic management maatregelen voor vaste en mobiele netwerken hetzelfde is.

2.4 Dimensie 3: Particuliere en zakelijke eindgebruikers

Transparantie over traffic management maatregelen is van belang voor zowel particuliere eindgebruikers (consumenten) als zakelijke eindgebruikers. Voor beide groepen geldt dat ze met het beschikbaar komen van meer informatie over zulke maatregelen een betere afweging kunnen maken in hun keuze tussen aanbiedingen van verschillende ISPs. Het eerder aangehaalde artikel 7.3 van het wetsvoorstel Telecommunicatiewet maakt ook geen onderscheid tussen particuliere en zakelijk gebruikers.

Dimensie 3: Een transparantieverplichting is aan de orde voor aanbieders die zich richten op particuliere eindgebruikers en voor aanbieders die zich richten op zakelijke eindgebruikers.

Een voor de hand liggende methode om de beoogde transparantie te verschaffen is het publiek beschikbaar maken van informatie over traffic management maatregelen via bijvoorbeeld websites en reclame-uitingen. In het volgende hoofdstuk wordt uitgebreid ingegaan op de manier waarop deze publieke beschikbaarheid van informatie naar verwachting het beste kan worden bereikt. Bij het verschaffen van transparante informatie aan zakelijke eindgebruikers is een kanttekening op zijn plaats. In de grootzakelijke markt verloopt de keuze tussen diensten van verschillende aanbieders op een andere manier dan in de consumentenmarkt en de kleinzakelijke markt. Aanbieders bedienen grote bedrijven vaak met maatwerkdiensten (“specials”). Gespecialiseerde inkopers bij de bedrijven maken een keuze tussen de diensten van verschillende aanbieders in (vaak uitgebreide) RFx[2] trajecten. Omdat het in dergelijke trajecten vaak om maatwerk gaat, is het in deze gevallen niet goed mogelijk om transparantie te verschaffen door het publiek bekend maken van informatie over traffic management maatregelen. Immers, deze maatregelen kunnen per aanbieding verschillen en bovendien vertrouwelijk zijn tussen de aanbieder en het afnemende bedrijf. De precieze kenmerken van de afgenomen diensten worden vaak vastgelegd in een Service Level Agreement (SLA) tussen aanbieder en bedrijf. Deze SLAs zullen ook vastleggen welke traffic management maatregelen de aanbieder toepast op het verkeer van het bedrijf, inclusief maatregelen die de toegang tot diensten voor het bedrijf kunnen beperken. Via het doorlopen van de RFx trajecten en het onderhandelen over de SLAs krijgt het afnemende bedrijf inzicht in de traffic

[2] RFx is een vaak gehanteerde verzamelterm voor RFI (Request for Information), RFP (Request for Proposal) en RFQ (Request for Quotation).

management maatregelen die het relevant vindt en de benaderingen die verschillende aanbieders op dit gebied hanteren.

Het hanteren van SLAs voor maatwerk aanbiedingen zoals hiervoor beschreven betekent uitdrukkelijk niet dat het verschaffen van transparantie door het publiek beschikbaar maken van informatie niet meer aan de orde is in de zakelijke markt. Ook maatwerk aanbiedingen aan bedrijven zijn vaak deels gebaseerd op standaard diensten die de betreffende aanbieder aan meerdere klanten levert. Voor diensten en dienstcomponenten die deel uitmaken van het standaard portfolio van de aanbieder is transparantie via het publiek beschikbaar maken van informatie een goede methode om eindgebruikers beter in staat te stellen hun afweging te maken tussen verschillende aanbieders. Het standaard portfolio beslaat hierbij alle standaard diensten die de aanbieder levert, aan zowel consumenten als zakelijke klanten.

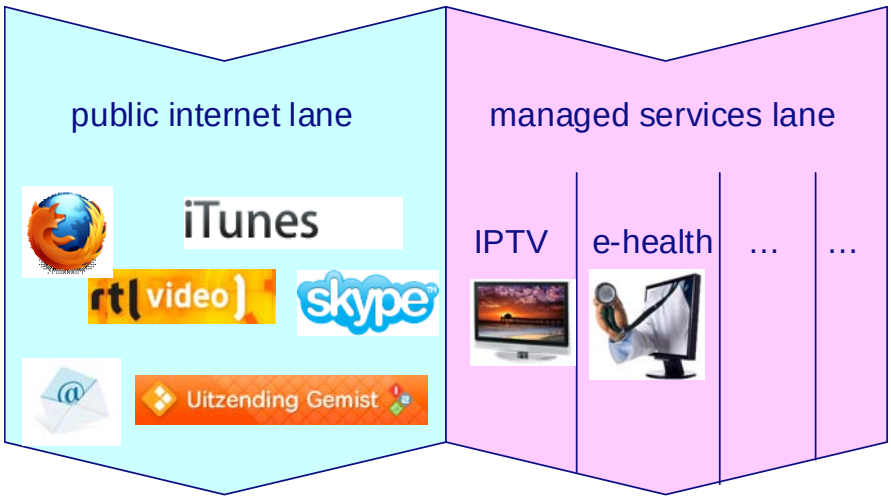
2.5 Dimensie 4: Effect van managed diensten op internettoegangsdienst

Aanvankelijk richtte de discussie over netwerkneutraliteit zich op het verschillend behandelen van verkeer over het publieke Internet. Het publieke Internet is een wereldwijd systeem van onderling verbonden netwerken die op basis van het IP protocol data vervoeren tussen aangesloten eindpunten. Er bestaat een rijke variëteit aan eindpunten, van PCs en mobiele terminals tot gespecialiseerde sensoren. Het woord “publiek” in publiek Internet benadrukt dat de eindgebruikers vanuit de eindpunten toegang hebben tot alle informatie en diensten die op het wereldwijde Internet beschikbaar zijn. Die informatie en diensten worden (eventueel tegen betaling) aangeboden door dienstaanbieders die zelf ook op een eindpunt op het publieke Internet zijn aangesloten. Het publieke Internet heeft hierin de rol van een transportnetwerk dat gebruikers en dienstaanbieders wereldwijd met elkaar verbindt. Het ondersteunt in principe alle diensten en applicaties door hun IP verkeer wereldwijd te transporteren tussen aanbieders en afnemers. ISPs spelen een belangrijke rol in het publieke Internet. Zij leveren de internettoegangsdienst: het stuk van de Internet keten tussen het huis- of bedrijfsnetwerk van de eindgebruiker en de Internet core (zie Figuur 4). Deze internettoegangsdienst is in het algemeen een zogenaamde ‘best-effort’ dienst. Zo is er geen garantie dat verzonden IP pakketten binnen een bepaalde tijd hun bestemming bereiken. Zo’n best-effort internettoegangsdienst sluit aan bij het best-effort karakter van de Internet core.

Aanbieders van internettoegangsdiensten leveren in toenemende mate ook andere IP gebaseerde diensten, vaak over dezelfde netwerkinfrastructuren maar in een aantal andere opzichten gescheiden van de ‘publieke’ internettoegangsdienst. Voorbeelden hiervan zijn de IPTV en IP telefonie diensten die door verschillende ISPs over hun DSL, kabel en glasnetwerken worden geleverd, in veel gevallen binnen één commerciële bundel met de internettoegangsdienst. Deze diensten worden meestal aangeduid als “managed services” [9]. Ze worden ook wel “managed or specialized services” [24] genoemd of omschreven als “additional, differentiated online services” [2]. De aanduiding “managed” is hier wat ongelukkig omdat het geen duidelijke afbakening oplevert ten opzichte van de internettoegangsdienst. Ook in de internettoegangsdienst en in het publieke Internet in het algemeen vinden verschillende vormen van management plaats die nodig zijn om het Internet efficiënt en betrouwbaar te laten werken. Daarnaast managen de aanbieders van diensten op het publieke Internet hun websites, app stores e.d. ook actief. In het algemeen is het wel zo dat de mate van diepgang en het niveau van garanties bij managed services verder gaat dan bij het best-effort publieke Internet.

Met het naast elkaar bestaan van (diensten over) publiek Internet en managed services ontstaat het zogenaamde two-lane model [23], zie Figuur 5. In dit two-lane model worden aan een

eindgebruiker over één breedband aansluiting (DSL, kabel, glas of mobiel) zowel de internettoegangsdienst als een aantal managed services geleverd.



Figuur 5. Two-lane model met internettoegang en managed services over één aansluiting

In de public Internet lane levert de ISP aan de eindgebruiker een internettoegangsdienst waarmee de eindgebruiker toegang krijgt tot de informatie en diensten op het publieke Internet. De gebruiker krijgt dus toegang tot een grote variëteit aan informatie en diensten op het Internet, terwijl hij van zijn ISP alleen de internettoegangsdienst afneemt. In een aantal gevallen zal de eindgebruiker met dienstaanbieders op het publieke Internet afspraken maken of een contract afsluiten. Deze afspraken gaan dan buiten de ISP om en vragen ook geen acties van de ISP. In de managed services lane levert de ISP op afspraak specifieke diensten aan de eindgebruiker. Deze afspraak over een specifieke dienst kan direct tussen de ISP en de eindgebruiker worden gemaakt, of via een afspraak tussen de eindgebruiker en een content provider, met een daaraan gerelateerde afspraak tussen de content provider en de ISP. Iedere specifieke dienst die een gebruiker op deze manier afneemt vraagt in het algemeen om een actie van de ISP. Meestal bestaat een deel van die actie uit het treffen van voorzieningen om de kwaliteit van de managed dienst te garanderen, bijvoorbeeld door bandbreedte te reserveren. In de public Internet lane worden geen voorzieningen per dienst getroffen om de kwaliteit te garanderen, de ISP levert hier een best-effort internettoegangsdienst. Tabel 1 vat de kenmerken van de public Internet lane en de managed services lane samen.

Tabel 1. Kenmerken van de public Internet lane en de managed services lane.

	public Internet lane	**managed services lane**
diensten geleverd door ISP	één dienst: toegang tot het wereldwijde publieke Internet	specifieke diensten, bijvoorbeeld IPTV, IP telefonie, …
afspraken tussen ISP en eindgebruiker	één afspraak over internettoegangsdienst	afspraak per dienst
kwaliteit	best effort (geen garanties)	typisch met gegarandeerde kwaliteit per dienst

De discussie over netneutraliteit beperkte zich aanvankelijk tot de public Internet lane. Met de opkomst van managed services, en de verwachting dat die in de toekomst in aantal en belang gaan groeien, wordt de discussie verbreed tot beide lanes ([9], [24]). Artikel 7.3 van het wetsvoorstel Telecommunicatiewet spreekt over "*eventuele beperkingen van de toegang tot of het gebruik van diensten en toepassingen*" en maakt daarbij geen onderscheid tussen de twee lanes. Toch lijkt het nuttig om bij het vormgeven van de transparantieverplichting wel een onderscheid te maken en de diepgang van de verplichting voor de managed services lane te beperken. Immers, bij de diensten die in de managed services lane worden geleverd verwacht een eindgebruiker in het algemeen al een aantal specifieke kenmerken en beperkingen bij de dienst, zoals een gegarandeerde HD kwaliteit en toegang tot een door het abonnement bepaald pakket kanalen bij een IPTV dienst. Dergelijke kenmerken en beperkingen liggen vast in de afspraken tussen de eindgebruiker en de ISP die de managed IPTV service levert. Een transparantieverplichting voor aanbieders op het gebied van de traffic management maatregelen die zij binnen hun managed services nemen voegt voor de gebruiker weinig toe en ligt daarom niet voor de hand. Aanbieders hoeven dus bijvoorbeeld niet transparant te zijn over de maatregelen die zij nemen om de kwaliteit van hun managed IP telefonie dienst te garanderen. Ook hoeven zij niet uit te leggen dat ze binnen deze managed dienst 112 noodoproepen voorrang geven boven de andere gesprekken.

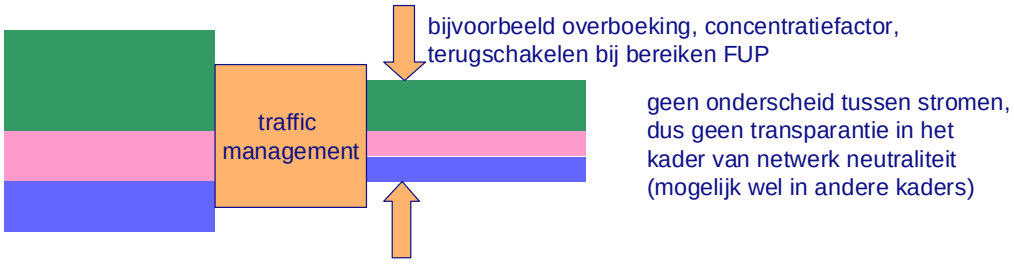
Tegelijkertijd kan de levering van managed services wel invloed hebben op de kwaliteit van de levering van diensten via de public Internet lane. Vaak worden de internettoegangsdienst en de managed services geleverd over één breedband infrastructuur, waarbij zij de capaciteit van dit netwerk delen. Managed services die om hun kwaliteit te garanderen gebruik maken van gegarandeerde capaciteit kunnen zo de capaciteit verkleinen die beschikbaar is voor de public Internet lane. Managed services kunnen zo de kwaliteit van diensten die eindgebruikers afnemen via de public Internet lane negatief beïnvloeden. Deze invloed is relevant voor eindgebruikers in hun keuze tussen ISPs die combinaties van de internettoegangsdienst en managed services leveren. Een geval waarin deze invloed duidelijk speelt is de situatie waarin dynamisch bandbreedte wordt gereserveerd voor een managed service (bijvoorbeeld een camerabewakingsdienst) ten koste van de bandbreedte in de public Internet lane. In dit geval kan een eindgebruiker merken dat op het moment dat de camerabewakingsdienst wordt ingeschakeld zijn downloads langer gaan duren doordat er minder bandbreedte voor beschikbaar is. Als dit effect van managed services op de public Internet lane bestaat dan is het nuttig en wenselijk dat de eindgebruiker hiervan op de hoogte is. In dit geval is een transparantieverplichting dus aan de orde. Bij statische (permanente) reservering van bandbreedte voor managed services is er geen invloed van de managed services op de public Internet lane. Het is mogelijk dat de statische bandbreedtereservering voor managed services speelt in een ander kader, bijvoorbeeld voortvloeiend uit de eerder genoemde motie Aasted Madsen-van Stiphout-Vos [14].

Dimensie 4: Een transparantieverplichting voor ISPs is aan de orde voor traffic management maatregelen die zij nemen in de internettoegangsdienst èn voor het effect dat de door hen geleverde managed services hebben op de internettoegangsdienst als geheel.

2.6 Dimensie 5: Onderscheid tussen verkeerstromen binnen de internettoegangsdienst

Binnen de in dit rapport gehanteerde context van netneutraliteit zijn niet alle traffic management maatregelen die in netwerken worden getroffen van belang. Het geven van transparantie is alleen aan orde als er traffic management maatregelen zijn die leiden tot het verschillend behandelen van verkeerstromen. In de in dit rapport gevolgde lijn hoeft dus geen

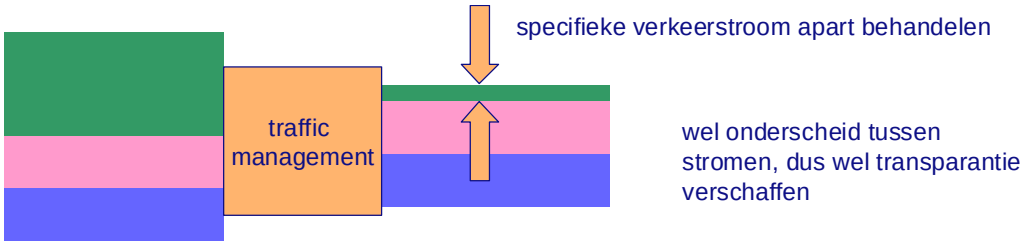
transparantie te worden verschaft over traffic management maatregelen die geen onderscheid maken tussen verschillende verkeerstromen. Zo vindt in veel ISP netwerken op meerdere plaatsen concentratie van verkeerstromen plaats, zoals geschetst in Figuur 6. Hierbij worden in concentratiepunten in het netwerk de verkeersstromen van verschillende gebruikers van de internettoegangsdienst geaggregeerd.



Figuur 6. Traffic management maatregelen die alleen op de totale verkeerstroom werken.

De bandbreedte beschikbaar voor de geaggregeerde verkeerstroom is daarbij in internettoegangsdiensten gericht op consumenten typisch een factor tien lager dan de gecombineerde bandbreedte van de individuele klanten. Bij deze concentratie wordt in de regel geen onderscheid gemaakt tussen verschillende typen verkeersstromen: alle stromen worden als dat nodig is met eenzelfde factor beperkt. Een ander voorbeeld is het beperken van de beschikbare bandbreedte van individuele klanten na het bereiken van een maximale hoeveelheid data volgens een Fair Use Policy (FUP). Daarbij wordt in de regel de totale bandbreedte voor een klant teruggebracht zonder onderscheid te maken tussen verschillende typen verkeersstromen. Voor deze typen van traffic management ligt een transparantieverplichting vanuit de in dit rapport gevolgde lijn niet voor de hand. Het is wel mogelijk dat er vanuit andere kaders transparantie moet worden geboden, bijvoorbeeld om de eindgebruikers een betere indruk te geven van de internetsnelheden die ze in de praktijk kunnen verwachten. Ook dit speelt in de eerder genoemde motie Aasted Madsen-van Stiphout-Vos [14].

Een transparantieverplichting is hier wel aan de orde wanneer specifieke verkeerstromen binnen de internettoegangsdienst een aparte behandeling krijgen, zie Figuur 7. De aparte behandeling kan bijvoorbeeld bestaan uit het herrouteren van de specifieke stroom (zoals streaming video in sectie 2.1.1) of het blokkeren van een specifieke stroom (zoals VoIP verkeer uit de use case in sectie 2.1.2). Ook de blokkeringen die gebeuren in een aantal bekende ISP diensten zoals SPAM filters en virusscanners vallen hieronder. Deze diensten worden door veel ISPs geleverd als vast onderdeel van hun internettoegangsdienst of als daaraan gekoppelde betaalde dienst.



Figuur 7. Traffic management maatregel die op een specifieke verkeersstroom binnen de totale stroom werkt.

In een aantal gevallen geven technische standaarden suggesties voor het onderscheid tussen verschillende verkeersklassen. Een voorbeeld is de 3GPP standaard TS 23.107 [25] die vier QoS klassen definieert in mobiel dataverkeer: conversational, streaming, interactive en background. Deze klassen zijn vooral gericht op traffic management maatregelen in mobiele radionetwerken, maar kunnen ook worden gekoppeld aan traffic management in de vaste delen van mobiele ISP netwerken. Mobiele ISPs kunnen ervoor kiezen bepaalde diensten of applicaties onder te brengen in verschillende QoS klassen en die QoS klassen vervolgens verschillend te behandelen in het netwerk. Ook in vaste netwerken zijn dit soort QoS benaderingen goed mogelijk, bijvoorbeeld op basis van DiffServ (RFC 2474 [26]). Voor dit type traffic management maatregelen is een transparantieverplichting aan de orde.

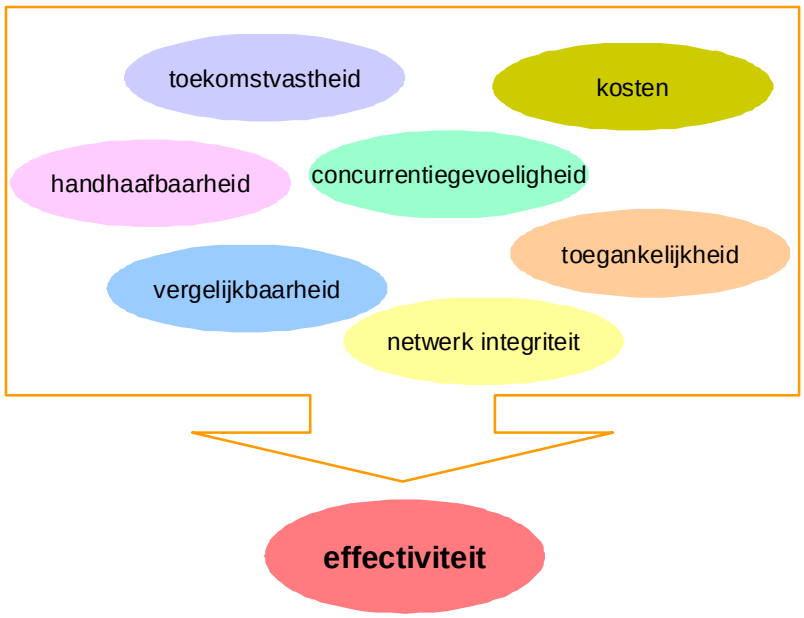
Dimensie 5: Een transparantieverplichting voor ISPs is aan de orde als ze traffic management maatregelen nemen die leiden tot het verschillend behandelen van verkeerstromen binnen de internettoegangsdienst. Traffic management maatregelen die alleen ingrijpen op de gehele verkeerstroom zonder onderscheid te maken tussen specifieke stromen daarbinnen worden in dit rapport buiten beschouwing gelaten.

3 Transparante informatie, betrokken partijen en processen

3.1 Eisen aan model

Transparantie over traffic management maatregelen in de context van netneutraliteit betekent dat ISPs informatie aan het publiek beschikbaar stellen over de technische maatregelen die ze in hun netwerken nemen om verschillende verkeerstromen op verschillende manieren te behandelen. Voor de inhoud, vorm en uitgebreidheid van deze informatie zijn vele mogelijkheden denkbaar. Dit hoofdstuk analyseert welke inhoud en vorm van de informatie het beste bijdragen aan het gewenste effect, namelijk een sturende werking richting ISPs, en tegelijkertijd voldoet aan een aantal bijkomende criteria zoals goede handhaafbaarheid, toekomstvastheid en beperkte kosten voor de betrokken marktpartijen. Dit betekent dat de vorm en inhoud van de informatie in nauwe samenhang met de betrokken partijen en de processen waarin ze een rol spelen wordt beschouwd. De combinatie van de informatie zelf, de partijen en de processen wordt in het vervolg van dit rapport aangeduid als het transparantiemodel.

De belangrijkste eis aan het model is dat het effectief is: de transparante informatie en de partijen en processen eromheen moeten inderdaad leiden tot de gewenste sturende werking richting ISPs. Naast deze hoofdeis bestaat een aantal andere eisen vanuit het wetsvoorstel Telecommunicatiewet en een aantal wensen vanuit de betrokken partijen en stakeholders zoals ISPs, content providers en consumentenorganisaties.



Figuur 8. Eisen aan het transparantiemodel.

Figuur 8 geeft een overzicht van de belangrijkste eisen die hieronder kort worden toegelicht.

- Toekomstvastheid is van belang omdat het model en de wettelijke regelingen waarin de transparantieverplichting wordt vastgelegd moeten kunnen omgaan met de snelle ontwikkelingen van diensten, netwerken en traffic management methoden. Het is in het

belang van ISPs, eindgebruikers en andere stakeholders dat de regels en de resulterende aanpak voor het ontstaan van transparantie voor langere tijd stabiel zijn.
- Handhaafbaarheid draagt bij aan de effectiviteit van de transparantieverplichting. Te verwachten valt dat OPTA een rol krijgt in de handhaving van de verplichting. Ook andere partijen en de Internet community in den brede kunnen een (signalerende) rol spelen in de handhaving. Voor een goede handhaving is het nodig dat OPTA toereikende en duidelijke informatie tot zijn beschikking heeft of kan krijgen over de traffic management maatregelen.
- Vergelijkbaarheid tussen traffic management informatie van verschillende aanbieders is nodig om eindgebruikers goed in staat te stellen een vergelijking en een keuze te maken tussen verschillende ISPs.
- Toegankelijkheid van de traffic management informatie is belangrijk voor de effectiviteit. Aan toegankelijkheid zitten verschillende kanten, zoals
  – De informatie moet eenvoudig vindbaar zijn op websites en in andere bedrijfsuitingen.
  – De informatie moet begrijpelijk zijn. Hierbij speelt dat begrijpelijkheid voor technisch onderlegde personen (“experts”) andere eisen stelt dan begrijpelijkheid voor de gemiddelde consument.
- Concurrentiegevoeligheid is een aandachtspunt dat vraagt om een afweging tussen de belangen van eindgebruikers en ISPs. Het doel van de transparantieverplichting is het bereiken van een sturend effect op ISPs voor wat betreft de traffic management maatregelen die zij inzetten. Het is goed denkbaar dat het invoeren van de transparantieverplichting er toe leidt dat traffic management een nieuw gebied wordt waarop ISPs met elkaar concurreren om de gunst van de eindgebruiker. Dit is een gewenst effect van de transparantieverplichting. Als echter van ISPs een verregaande mate van detail in hun informatie over traffic management maatregelen wordt geëist, kan dat leiden tot een situatie waarin ISPs onnodig diepgaand inzicht krijgen in de precieze dimensionering en operationeel beheer van de netwerken van hun concurrenten. Dit is niet de bedoeling van de transparantieverplichting.
- Netwerkintegriteit is een aandachtspunt dat ook gekoppeld is aan de mate van detail in de informatie die van ISPs gevraagd wordt. Een grote mate van detail kan kwaadwillenden inzicht geven in mogelijke kwetsbaarheden in de beveiliging van netwerken en diensten.

De bovenstaande eisen liggen aan de basis van het door TNO voorgestelde transparantiemodel, beschreven in de volgende paragrafen. Bij het maken van dit model is ook gebruik gemaakt van de reacties en suggesties van de deelnemers aan de twee workshops die in het kader van dit onderzoek zijn gehouden.

3.2 Model op hoofdlijnen

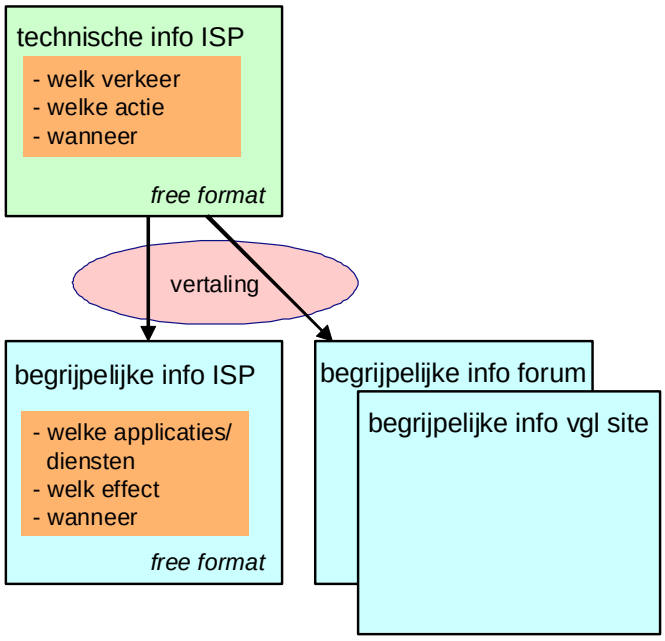
3.2.1 Technische en begrijpelijke informatie

De eisen die aan het transparantiemodel en de informatie over traffic management maatregelen worden gesteld lopen sterk uiteen. Het is daardoor lastig om met één soort informatie binnen het model aan de combinatie van eisen te voldoen. Het hier voorgestelde model is daarom gebaseerd op twee soorten informatie, gericht op verschillende doelgroepen: technische informatie en begrijpelijke informatie.
- De technische informatie beschrijft in technische termen de traffic management maatregelen die een ISP instelt. Voor experts biedt dit een duidelijke toegang tot de

feitelijke technische maatregelen. Voor de gemiddelde eindgebruiker is de technische informatie wellicht minder bruikbaar.
- De begrijpelijke informatie beschrijft de gevolgen van de traffic management maatregelen voor de eindgebruikers, in termen die een brede groep eindgebruikers begrijpt.

Deze tweedeling in soorten informatie gebeurt dus vanuit het perspectief van de gemiddelde eindgebruiker die moeite zal hebben om de technische informatie te interpreteren. Voor technische experts is ook de technische informatie begrijpelijk.

Figuur 9 toont de hoofdlijnen van het transparantiemodel met deze twee soorten informatie. De basis van het model wordt gevormd door de technische informatie, die vervolgens wordt vertaald naar begrijpelijke informatie.



Figuur 9. Transparantiemodel met technische en begrijpelijke informatie.

De technische informatie bevat per traffic management maatregel die binnen de in het vorige hoofdstuk beschreven reikwijdte valt drie elementen:

1. Welke verkeerstroom wordt door traffic management maatregelen speciaal behandeld?
2. Welke maatregel wordt toegepast op deze verkeerstroom?
3. Wanneer wordt deze maatregel toegepast?

Paragraaf 3.3 gaat in op de mate van detail en preciezere soorten informatie die voor deze drie elementen wordt voorgesteld.

De technische informatie is direct van nut voor experts die de traffic management maatregelen van ISPs willen analyseren. Daarnaast is het de basis voor de vertaling naar begrijpelijke informatie, mogelijk door dezelfde experts. De ISPs zijn in de beste positie om de technische informatie beschikbaar te stellen, omdat zij zelf bepalen welke traffic management maatregelen zij hanteren in hun internettoegangsdienst. Gezien de belangrijke rol van technische informatie ligt het in de rede om ISPs te verplichten de technische informatie over de traffic management maatregelen die ze in hun netwerk nemen beschikbaar te maken. Door het opnemen van de hierboven genoemde drie elementen in de verplichting ontstaat ook een technische vergelijkbaarheid tussen traffic management maatregelen van verschillende ISPs.

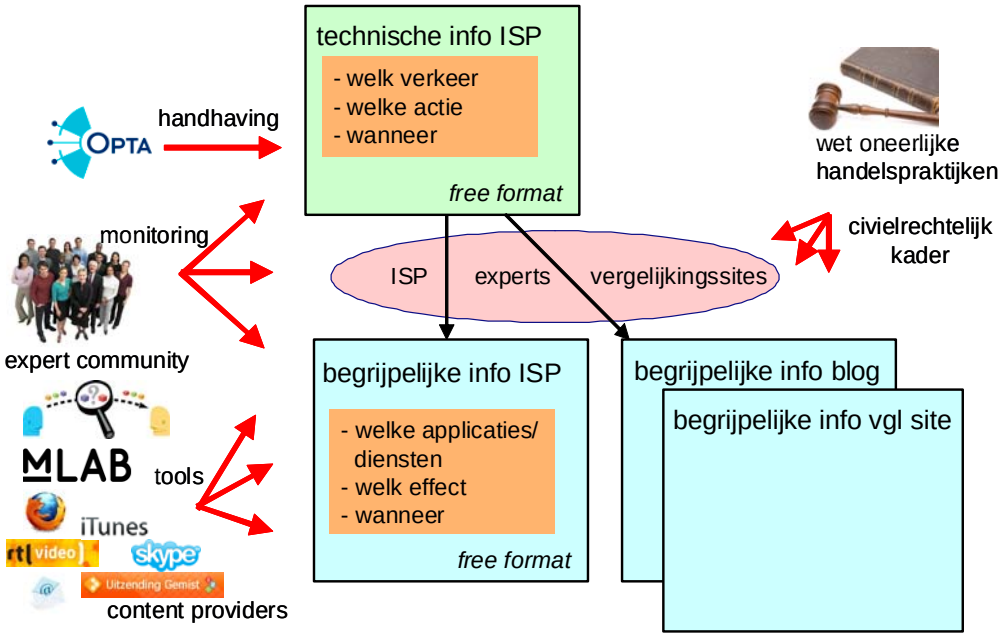
De begrijpelijke informatie ontstaat door een vertaling van de technische informatie over traffic management maatregelen naar de belevingswereld van de eindgebruiker. De begrijpelijke informatie beschrijft:

- Welke applicaties en diensten een speciale behandeling krijgen.
- Wat het effect van de speciale behandeling is of kan zijn op de beleving van de dienst door de eindgebruiker.
- Wanneer dit effect merkbaar is.

Zoals later wordt uitgelegd in sectie 3.4, is de vertaling van de drie elementen uit de technische informatie naar de hierboven genoemde elementen op hoofdlijnen relatief eenvoudig maar deels subjectief. Dit is één van de overwegingen waarom een verplichting aan ISPs om begrijpelijke informatie te publiceren niet voor de hand ligt.

3.2.2 Rollen van marktpartijen en stakeholders

Net zo belangrijk als de technische en begrijpelijke informatie in het model is de manier waarop marktpartijen en stakeholders een rol spelen bij het opstellen, interpreteren, vertalen en controleren van de informatie. Figuur 10 geeft een overzicht van de interacties van een aantal relevante marktpartijen en stakeholders in het model.



Figuur 10. Rollen van marktpartijen en stakeholders in het transparantiemodel.

- Een belangrijke rol is uiteraard weggelegd voor de ISPs. In het model zijn zij verplicht om technische informatie te verschaffen over de traffic management maatregelen die zij nemen, voor zover die binnen de in het vorige hoofdstuk beschreven reikwijdte vallen. Daarnaast zullen de ISPs waarschijnlijk de behoefte voelen om de technische informatie verder toe te lichten aan hun (potentiële) klanten, door de vertaling te maken naar voor hen begrijpelijke informatie.
- De publieke beschikbaarheid van technische informatie stelt ook andere partijen, zoals vergelijkingssites, in staat om deze informatie te publiceren en daarbij ook een vertaling naar begrijpelijke informatie te maken. Hiermee kunnen er voor eindgebruikers verschillende bronnen van begrijpelijke informatie beschikbaar komen. Omdat de

begrijpelijke informatie, zoals uitgelegd in sectie 3.4, naar zijn aard subjectief is, kunnen er verschillen van inzicht en discussies ontstaan over de juistheid van de vertaling. Dergelijke discussies over het effect van traffic management maatregelen op de dienstbeleving bij de eindgebruiker zijn op zich geen probleem. Ze zorgen voor extra aandacht voor netneutraliteit en de rol van traffic management maatregelen daarbinnen. Hierdoor kunnen ze bijdragen aan het gewenste sturende effect van de transparantieverplichting op ISPs. Marktpartijen en belanghebbenden die zich benadeeld voelen door gepubliceerde informatie kunnen gebruik maken van de bestaande civielrechtelijke middelen, in het bijzonder de Wet Oneerlijke Handelspraktijken.

- OPTA zal waarschijnlijk gaan toezien op de correcte naleving van de transparantieverplichting. Deze handhaving zal zich toespitsen op de correctheid en volledigheid van de technische informatie die verplicht verschaft wordt door ISPs. Zoals later beschreven in sectie 3.4 volgt de begrijpelijke informatie op hoofdlijnen relatief eenvoudig uit de technische informatie, maar is de daarbij gebruikte vertaling deels subjectief. Het handhaven van de correctheid van de begrijpelijke informatie door OPTA ligt daarom niet voor de hand. Dit is ook een belangrijke overweging om geen verplichting in te stellen voor het beschikbaar stellen van begrijpelijke informatie. Immers, dit zou leiden tot een verplichting die lastig of niet te handhaven is. Zoals beschreven in sectie 3.4 zijn er ook andere overwegingen om geen verplichting voor het beschikbaar stellen van begrijpelijke informatie in te voeren.
- Traditioneel is op het Internet een stevige rol weggelegd voor de zogenaamde expert community. Vanuit deze community worden nationale en internationale ontwikkelingen in netwerken en diensten nauwlettend gevolgd. Experts uit de community kunnen de technische informatie geleverd door de ISPs analyseren, vergelijken, becommentariëren en vertalen naar begrijpelijke informatie. De begrijpelijke informatie opgesteld door de experts kan via fora en blogs beschikbaar komen voor het brede publiek. Daarnaast zullen de experts waarschijnlijk ook een controlerende rol op zich nemen. Zo kunnen ze met publiek beschikbare tools zoals M-lab [27] de correctheid en volledigheid van (delen van) de technische informatie geleverd door ISPs toetsen. In aanvulling op de monitoring activiteiten van de Internet community is het goed denkbaar dat ook de Nederlandse overheid de situatie rondom traffic management maatregelen gaat (laten) monitoren. Voor EL&I geeft dit inzicht in de mate waarin de transparantieverplichting zijn gewenste effect in de markt heeft. Daarnaast kan de monitoring nuttige informatie opleveren voor de handhaving van de verplichting door OPTA.
- Ook vergelijkingssites kunnen analyses maken van de beschikbare technische informatie en die voor hun bezoekers vertalen naar begrijpelijke informatie. Voor veel eindgebruikers vormen vergelijkingssites een belangrijke bron van informatie die ze raadplegen bij hun keuze tussen verschillende aanbiedingen voor internettoegang.
- Naast de expert community zullen ook content providers en dienstaanbieders de door de ISPs geleverde technische informatie bestuderen en deze in gevallen willen vertalen naar wat de traffic management maatregelen betekenen voor de gebruikers van hun diensten.

3.3 Technische informatie: verplichting voor ISPs

De technische informatie beschrijft in technische termen de traffic management maatregelen die een ISP instelt. Deze informatie biedt voor experts een duidelijke toegang tot de feitelijke technische maatregelen. De technische informatie is opgedeeld in de drie eerder genoemde elementen (“welk verkeer”, “welke maatregelen” en “wanneer”) die nodig zijn om de beoogde transparantie voor experts te bereiken. De volgende paragrafen bespreken in meer detail welke informatie per element aan de orde is.

In het algemeen kunnen meerdere traffic management maatregelen tegelijkertijd worden toegepast. Voor het verkrijgen van een volledig beeld is het nodig dat voor iedere traffic management maatregel (voor zover die binnen de in het vorige hoofdstuk beschreven reikwijdte valt) de technische informatie beschikbaar is. Als de traffic management maatregelen verschillen tussen abonnementsvormen is het nodig dat een uitsplitsing beschikbaar is waaruit blijkt welke maatregelen per abonnementsvorm van toepassing zijn.

3.3.1 Welk verkeer: twee niveaus

Om transparantie te kunnen bieden over een traffic management maatregel zal duidelijk beschreven moeten worden welk verkeer eraan onderhevig is. Bij deze beschrijving zijn twee niveaus te onderscheiden, waarbij het voorstel is om het eerste niveau van informatie verplicht te stellen en het tweede, meer gedetailleerde niveau niet.

3.3.1.1 Niveau A: klassen van toepassingen en technische parameters

Niveau A geeft een omschrijving van het verkeer in termen van
"Verkeersstromen afkomstig van/bestemd voor (klassen van) ***toepassingen*** *inclusief de opsomming van de (combinaties van)* ***technische parameters*** *die het verkeer karakteriseren, zoals URL, domeinnaam, IP adres, protocol, poort nummer, AS nummer, peering partners, terminal typen, …"*

Bij de technische parameters gaat het bij dit niveau alleen om het *gebruik* van de parameters in de selectie van het verkeer, niet om de *waarden* van de parameters die worden gebruikt. Voor de drie eerder in paragraaf 2.1 ingevoerde use cases ziet de technische informatie op niveau A er bijvoorbeeld als volgt uit:

- Efficiënter afleveren streaming video: *"streaming video verkeer met daarin populaire content van bepaalde Internet dienstaanbieders op basis van de URL van hun website"*
- VoIP verkeer op mobiele netwerken blokkeren,
  - optie a): *"VoIP verkeer over het mobiele netwerk, geselecteerd op basis van verschillende combinatie van IP bestemmingsadres en gebruik van het SIP protocol"*
  - optie b): *"VoIP verkeer over het mobiele netwerk, geselecteerd op de combinatie van het gebruik van bepaalde applicaties op de mobiele terminal en een mobiele verbinding"*
- Tijdkritische applicaties voorrang geven bij congestie: *"real-time en interactief verkeer, geselecteerd op basis van het gebruik van het http, SIP of RTP protocol"*

Het hier gedefinieerde niveau A is in het algemeen het minimale niveau van informatie dat technische experts nodig hebben om te kunnen inschatten welk verkeer wel en welk verkeer niet aan traffic management onderhevig is. Als het onderdeel ***technische parameters*** wordt weggelaten verdwijnt in de tweede use case bijvoorbeeld het onderscheid tussen de geschetste methoden om VoIP verkeer over mobiele netwerken te blokkeren. In de derde use case blijft onduidelijk welke verkeerstromen onder de noemer real-time en interactief verkeer zouden kunnen vallen. Met het ontbreken van deze informatie is het voor technische experts niet meer goed mogelijk om een vertaling naar zinvolle begrijpelijke informatie te maken.

De informatie over technische parameters is ook nodig als aanknopingspunt voor de handhaving. De handhaving zal deels worden gestuurd door klachten van eindgebruikers die vermoeden dat de prestaties van bepaalde applicaties negatief worden beïnvloed door traffic management maatregelen. Zonder de technische parameter informatie is het voor de handhavende instantie veelal onmogelijk om te beoordelen of een applicatie onder een

gepubliceerde traffic management maatregelen valt, of dat er sprake is van een andere, niet gepubliceerde maatregel.

Voor ISPs kan de detaillering die ontstaat door de informatie over technische parameters te verstrekken ook nuttig zijn omdat ze daarmee het bereik van hun maatregelen preciezer kunnen aangeven. Zonder de technische informatie over parameters kan bijvoorbeeld onbedoeld de indruk ontstaan dat de traffic maatregelen gelden voor brede klassen applicaties, terwijl ze alleen worden toegepast op een kleinere, preciezer te omschrijven groep.

De technische informatie op niveau A is dus nodig voor zinvolle interpretatie van de traffic management maatregelen door experts en voor het creëren van voldoende aanknopingspunten voor de handhaving. Het voorstel is daarom om ISPs te verplichten de informatie binnen niveau A beschikbaar te maken.

3.3.1.2 Niveau B: klassen van toepassingen, technische parameters en hun waarden

Niveau B gaat een stap verder dan niveau A door de toevoeging van de waarden van de parameters die worden gebruikt voor het selecteren van het verkeer.

> Niveau B geeft een omschrijving van het verkeer in termen van
> *"Verkeersstromen afkomstig van/bestemd voor (klassen van)* ***toepassingen*** *inclusief de opsomming van de (combinaties van)* ***technische parameters*** *die het verkeer karakteriseren, zoals URL, domeinnaam, IP adres, protocol, poort nummer, AS nummer, peering partners, terminal typen, … met opgave van de* ***specifieke waarden van de parameters*** *die het verkeer karakteriseren"*

Voor de drie use cases ziet de technische informatie op niveau B er bijvoorbeeld als volgt uit:

- Efficiënter afleveren streaming video: *"streaming video verkeer met daarin populaire content van bepaalde Internet dienstaanbieders op basis van de URL van hun website. De betreffende URLs zijn uitzendingengemist.be, thevideoarchiver.net en nationalevideo.nl."*
- VoIP verkeer op mobiele netwerken blokkeren,
  - optie a): *"VoIP verkeer over het mobiele netwerk, geselecteerd op basis van verschillende combinatie van IP bestemmingsadres en gebruik van het SIP protocol. De lijst met IP adressen is per 15 november 2010: 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."*
  - optie b): *"VoIP verkeer over het mobiele netwerk, geselecteerd op de combinatie van het gebruik van bepaalde applicaties op de mobiele terminal en een mobiele verbinding. De betrokken applicaties per 1 november 2010 zijn VoIPXpress, Zceip, InetPhone, Speakerz, VoiceXpresser."*
- Tijdkritische applicaties voorrang geven bij congestie: *"real-time en interactief verkeer, geselecteerd op basis van het gebruik van het http, SIP of RTP protocol"*

De onderstreepte zinsneden hierboven zijn de toevoegingen ten opzichte van niveau A. Merk op dat in de derde use case parameterwaarden geen rol spelen. Niveau B voegt daardoor in dit geval geen informatie toe aan niveau A.

Technische experts kunnen met de niveau B informatie tot in grote mate van detail controleren of de door de ISPs verschafte transparante informatie correct is. Ook in de handhaving kan de niveau B informatie waardevol zijn in gevallen waarin een diepgaande

analyse van de traffic management maatregelen aan de orde is. Tegelijkertijd is het twijfelachtig of de niveau B informatie bijdraagt aan betere of completere begrijpelijke informatie voor de gemiddelde eindgebruiker. De bijdrage van de niveau B informatie aan de effectiviteit van de transparantieverplichting, die voor een groot deel wordt bepaald door begrijpelijke informatie, is hiermee in het algemeen beperkt.

Voor ISPs betekent het vermelden en actueel houden van de niveau B informatie substantieel meer werk dan zij moeten doen voor niveau A. Daarnaast geeft de niveau B informatie potentieel veel informatie over de manier waarop ze hun netwerken en diensten inrichten. Het is in het algemeen niet te bepalen of de niveau B informatie hiermee concurrentiegevoelig is of een bedreiging voor de netwerkintegriteit kan opleveren, omdat dit sterk afhangt van de precieze informatie. Concurrentiegevoeligheid en netwerkintegriteit zijn wel duidelijke aandachtspunten bij niveau B.

Gegeven de waarschijnlijk beperkte bijdrage van de niveau B informatie aan de effectiviteit van de transparantieverplichtingen, het extra werk dat van ISPs gevraagd wordt en de mogelijke issues rondom concurrentiegevoeligheid en netwerkintegriteit ligt het niet voor de hand om ISPs te verplichten om de informatie van niveau B publiek beschikbaar te stellen.

Zoals hierboven opgemerkt kan de informatie van niveau B wel een waardevolle rol spelen in de handhaving van de transparantieverplichting. Hierbij is goed voorstelbaar dat een ISP in het kader van een specifieke handhavingsactie de niveau B informatie wel binnen een vertrouwelijke context aan de toezichthoudende instantie ter beschikking stelt. De omvang van de informatie kan daarbij beperkt blijven tot de informatie die nodig is om in het specifieke geval een gedetailleerde analyse te doen. De vertrouwelijke context zorgt er daarbij voor dat recht wordt gedaan aan de mogelijke concurrentiegevoeligheid en het belang van netwerkintegriteit.

Uiteraard staat het ISPs vrij om in gevallen waarin dat nuttig is wel te kiezen voor het publiek maken van de niveau B informatie. In het geval van de eerste use case over streaming video bijvoorbeeld kan een ISP overwegen om de URLs van de betrokken videodiensten wel te noemen. De lijst met URLs kan goed worden opgenomen in begrijpelijke informatie en daarbij extra inzicht geven aan eindgebruikers in het effect van de traffic management maatregel. Ook voor de ISP zelf kan het publiek maken van de lijst van betrokken URLs nuttig zijn, bijvoorbeeld om mogelijke speculaties in de markt te voorkomen over de vraag welke videodiensten wel en welke niet speciaal worden behandeld. Binnen het hier voorgestelde model met alleen een verplichting voor informatie op niveau A wordt de afweging over het publiek maken van aanvullende informatie overgelaten aan de ISPs. De verwachting is dat de ISPs in hun overwegingen hierbij ook rekening houden met de vragen die bij andere partijen en eindgebruikers ontstaan naar aanleiding van de niveau A informatie.

3.3.2 Welke maatregel

Naast de karakterisering van het verkeer dat onderhevig is aan een traffic management maatregel is uiteraard nodig te weten wat de maatregel inhoudt. Dit element van de technische informatie laat zich omschrijven als:

> “de technische maatregelen waarmee de betreffende verkeerstroom afwijkend wordt behandeld ten opzichte van andere verkeerstromen binnen de internettoegangsdienst”

De beschrijving van de maatregel moet in technische termen en waar mogelijk kwantitatief worden geformuleerd. Er bestaat een grote variëteit aan opties om maatregelen op verkeersstromen technisch in netwerken te implementeren. In de praktijk vallen de meeste maatregelen in één van de volgende categorieën:

- De verkeersstroom blokkeren, pakketten "droppen" (verwijderen). Bij dit type maatregelen is een kwalitatieve beschrijving in het algemeen voldoende.
- Beperken van de bandbreedte. Hierbij is het nodig uit te leggen wat de kwantitatieve gevolgen voor de bandbreedte zijn.
- Hanteren verschillende prioriteiten, zoals de eerder genoemde 3GPP QoS klassen en DiffServ code points. Hierbij is een uitsplitsing van verkeersstromen over de verschillende prioriteiten nodig.
- Routeren over apart deel netwerk. Hierbij is het nodig uit te leggen wat deze routering inhoudt en hoe en in welke mate het aparte deel van het netwerk anders is dan het deel dat voor het overige verkeer wordt gebruikt.
- Herrouteren naar andere bestemmingen. Dit vraagt om een beschrijving van de nieuwe bestemming en een uitleg hoe die zich verhoudt tot de oorspronkelijke bestemming.
- Ingrijpen in verkeersstroom zelf. Hierbij moet duidelijk worden gemaakt welke veranderingen worden aangebracht in het verkeer, bijvoorbeeld door het weglaten, toevoegen en veranderen van bepaalde pakketten.

Voor de drie use cases kan deze informatie er als volgt uitzien:

- Efficiënter afleveren streaming video: *"De video stream wordt vanuit aparte caches binnen ons eigen netwerk geleverd in plaats van vanuit het netwerk van de dienstleverancier. Hierdoor wordt de video stream via een kortere route geleverd. De content zelf verandert hierbij niet."*
- VoIP verkeer op mobiele netwerken blokkeren,
  - optie a): *"Het betreffende verkeer wordt geblokkeerd."*
  - optie b): *"De betreffende applicaties op de mobiele terminal staan geen VoIP sessies over mobiele verbindingen toe."*
- Tijdkritische applicaties voorrang geven bij congestie: *"Het betreffende verkeer wordt in de "streaming" QoS klasse ingedeeld en krijgt voorrang op het overige verkeer dat wordt ingedeeld in de "background" klasse."*

3.3.3 Wanneer

Het laatste element van de technische informatie gaat in op de vraag wanneer de traffic management maatregel actief is. In het eenvoudigste geval gaat het hier om specifieke tijdstippen. Een andere belangrijke categorie maatregelen wordt waarschijnlijk niet toegepast op vooraf bekende tijdstippen maar onder specifieke omstandigheden zoals congestie in het netwerk. Ook combinaties van omstandigheden en tijdselementen zijn mogelijk, zoals "*na het bereiken van de P2P datalimiet van 10 Gigabyte per maand*".

De bij het derde element van de technische informatie gevraagde informatie laat zich hiermee omschrijven als:

"de tijdstippen waarop of specifieke omstandigheden waaronder de genoemde technische maatregelen op de genoemde verkeerstromen worden toegepast"

Voor de drie use cases kan deze informatie als volgt uitzien:

- Efficiënter afleveren streaming video: *"Altijd"*

- VoIP verkeer op mobiele netwerken blokkeren, optie a) en b): *"Altijd op mobiele netwerken"*
- Tijdkritische applicaties voorrang geven bij congestie: *"Tijdens congestie in specifieke cellen in het mobiele netwerk"*

3.3.4 Presentatie van technische informatie

3.3.4.1 Geen voorgeschreven formaat

De voorgaande paragrafen geven een overzicht van de soorten technische informatie die in het voorgestelde model onder de transparantieverplichting voor ISPs vallen. De daarop volgende vraag is welk formaat of vorm voor het publiceren van de informatie het best bijdraagt aan de effectiviteit van de transparantieverplichting. Het voorstel in dit rapport is om de elementen die ISPs moeten opnemen in hun technische informatie over traffic management maatregelen voor te schrijven, maar geen specifiek formaat of vorm voor het publiceren van de informatie op te leggen. De belangrijkste overweging om geen formaat voor te schrijven, is dat het aantal mogelijke traffic management maatregelen en de (klassen van) applicaties waarop deze invloed hebben erg groot is. Het is erg lastig om tot een formaat te komen dat in het overgrote deel van de gevallen bruikbaar en zinnig is. Dit blijkt al uit de drie use cases in de voorgaande paragrafen. De eis van toekomstvastheid betekent daarbij dat een dergelijk formaat ook nog toepasbaar moet zijn op nu nog onbekende traffic management maatregelen die in de toekomst ontwikkeld gaan worden.

Een andere reden om niet voor een vast formaat te kiezen is dat het de mogelijkheden voor ISPs kan beperken om zich van elkaar te onderscheiden op het gebied van traffic management maatregelen. Deze overweging heeft bij het opstellen van een andere transparantieverplichting voor telefonie tarieven ook geleid tot het vastleggen van een aantal verplichte informatie-elementen in combinatie met een vrij formaat [28].

Een argument voor een vast formaat is dat het bijdraagt aan de vergelijkbaarheid van informatie voor eindgebruikers. Als eindgebruikers de informatie van verschillende ISPs beter kunnen vergelijken, draagt dat weer bij aan de effectiviteit van de transparantieverplichting. Voor de technische informatie waar het hier over gaat is het verwachte effect van de vergelijkbaarheid echter beperkt. Immers, voor de meeste eindgebruikers is de technische informatie beperkt bruikbaar. Voor hen is vergelijkbaarheid vooral bij de begrijpelijke informatie van belang. Zoals beschreven in paragraaf 3.4.2 kan voor deze informatie op verschillende manieren vergelijkbaarheid ontstaan.

Het vrije formaat stelt ISPs in staat om de technische informatie in samenhang met begrijpelijke informatie te presenteren. Deze benadering is in de praktijk te zien bij een aantal Canadese ISPs ([21], [22]). In Canada was tijdens het schrijven van dit rapport al een transparantieverplichting voor traffic management maatregelen van kracht [6].

3.3.4.2 Vindbaarheid en actualiteit

Voor de effectiviteit van de transparantieverplichting is het van belang dat de informatie goed en makkelijke vindbaar is op ISP websites, bijvoorbeeld samen met andere informatie over de aangeboden internettoegangsdiensten, zoals prijs en bandbreedte. Hoewel er binnen het hier voorgestelde model alleen verplichtingen gelden voor de technische informatie heeft deze verplichting naar verwachting een duidelijke uitstraling naar de begrijpelijke informatie die beschikbaar komt. Immers, zoals beschreven in paragraaf 3.4.2 zullen ISPs

hoogstwaarschijnlijk de technische informatie willen toelichten aan hun (potentiële) klanten door een vertaling te maken naar begrijpelijke informatie.

De informatie moet niet alleen goed vindbaar maar ook voldoende actueel zijn. De actualiteit van de informatie is van belang in twee situaties waarin eindgebruikers behoefte kunnen hebben aan informatie over traffic management maatregelen:

- Voor eindgebruikers die internettoegangsdiensten van verschillende ISPs vergelijken is het van belang dat de informatie waarop ze hun overwegingen baseren up to date is en liefst nog een zekere tijd geldig blijft.
- Een bepaalde groep eindgebruikers zal op de hoogte willen zijn van nieuwe of veranderende traffic management maatregelen binnen hun bestaande internettoegangsdienst die de voor hen belangrijke toepassingen (kunnen) gaan raken. Voor hen is het nuttig als er een zekere tijd zit tussen de aankondiging en de invoering van een nieuwe of veranderde maatregel zodat ze niet verrast worden door toepassingen die plotseling in kwaliteit veranderen.

Het voorstel hier is om ISPs te verplichten om nieuwe traffic management maatregelen en veranderingen in bestaande maatregelen ten minste vier weken voordat ze van kracht worden aan te kondigen op hun website. Deze termijn van vier weken wordt ook gehanteerd in artikel 7.2 van de Telecommunicatiewet over het informeren van eindgebruikers over wijzigingen in de contractuele voorwaarden van diensten.

Bij nieuwe traffic management maatregelen en veranderingen in bestaande maatregelen kan de vraag aan de orde zijn of er sprake is van een verandering in de dienstvoorwaarden in het nadeel van de eindgebruiker. Zo'n verandering in de voorwaarden kan de eindgebruiker het recht geven om zijn abonnement kosteloos te beëindigen. Of en in welke mate er sprake is van een verslechtering van de voorwaarden voor de eindgebruiker hangt af van de applicaties die een eindgebruiker veel gebruikt en belangrijk vindt. Merk op dat traffic management maatregelen ook juist kunnen leiden tot een verbetering van de beleving van diensten door de eindgebruiker.

3.4 Begrijpelijke informatie

3.4.1 Subjectieve vertaling vanuit technische informatie

De voor de gemiddelde eindgebruiker begrijpelijke informatie ontstaat door vertaling van de technische informatie naar de belevingswereld van de eindgebruiker. Op hoofdlijnen is deze vertaling relatief eenvoudig. De begrijpelijke informatie draait in essentie om de drie elementen die al genoemd werden in paragraaf 3.2.1. Deze elementen staan in nauw verband met de door de ISP verplicht te verschaffen technische informatie:

- Welke applicaties en diensten krijgen een speciale behandeling?
  De applicaties en diensten worden bepaald door de selectie van de verkeerstromen die vanuit traffic management een speciale behandeling krijgen.
- Wat is of kan het effect zijn van de speciale behandeling op de dienstbeleving van de eindgebruiker?
  Het effect hangt af van de precieze acties die vanuit traffic management worden toegepast op de geselecteerde verkeersstromen.
- Wanneer is dit effect merkbaar?
  Het effect is merkbaar wanneer de traffic management maatregelen actief zijn.

De vertaling is hiermee op hoofdlijnen in de meeste gevallen eenvoudig uit te voeren. Tegelijkertijd is de vertaling vaak subjectief, doordat naast de traffic management maatregelen ook andere factoren invloed kunnen hebben op de dienstbeleving van de eindgebruiker. Hierbij gaat het bijvoorbeeld om de invloed van de andere netwerkdelen in de keten (Figuur 4). Deze factoren kunnen het effect van de traffic management maatregelen (deels) verhullen of juist versterkt tot uitdrukking laten komen. Een andere oorzaak van de subjectiviteit van de vertaling is dat de gebruikersbeleving afhangt van de verwachting die een eindgebruiker zich vooraf heeft gevormd over de kwaliteit van een dienst. Deze verwachting verschilt van gebruiker tot gebruiker. De vertaling van technische naar begrijpelijke informatie en de subjectiviteit daarin wordt hieronder toegelicht aan de hand van de drie eerder ingevoerde use cases.

Efficiënter afleveren streaming video

- *Welke applicaties en diensten?* In deze use case is duidelijk dat videodiensten kunnen profiteren van de traffic management maatregel. Deze informatie is op zich al nuttig voor eindgebruikers: afhankelijk van of ze veel video kijken of niet kan deze maatregel hun dienstbeleving meer of minder beïnvloeden. Zoals beschreven in paragraaf 3.3.1.2 kan de ISP ervoor kiezen om ook de URLs van de betreffende videodiensten en websites te vermelden. Dit biedt eindgebruikers een gedetailleerder inzicht. Als de ISP deze informatie beschikbaar maakt op zijn website kan deze ook worden gebruikt door andere partijen die begrijpelijke informatie publiceren.
- *Welk effect?* Het effect dat de eindgebruiker merkt is in het algemeen lastig te omschrijven. Als het ISP netwerk flink belast is, kunnen de streams van de betrokken videodiensten met een hogere kwaliteit worden afgeleverd dan streams van andere videodiensten, doordat ze een kortere weg door het netwerk afleggen en daardoor minder last hebben van congestie. Deze kwaliteitsverhoging hangt dan wel af van de precieze verdeling van de verkeerstromen en congestieproblemen over het netwerk op het moment van kijken. Bij een relatief lage belasting kan het goed zijn dat er nauwelijks een effect op de gebruikerservaring is, doordat alle video streams goed worden afgeleverd. Het interessante aan deze traffic management maatregel is dat het verbeteren van de kwaliteit van de betrokken videodiensten niet ten koste hoeft te gaan van overige video- en andere internetdiensten. Het ontlasten van het netwerk door de populaire video's te cachen kan de dienstbeleving van de andere diensten juist verbeteren, weer afhankelijk van de precieze verdeling van de verkeersstromen over het netwerk.
- *Wanneer?* De "wanneer" vraag is wel eenvoudig te beantwoorden: altijd.

VoIP verkeer op mobiele netwerken blokkeren

- *Welke applicaties en diensten?* In de "VoIP verkeer blokkeren" use case speelt de vraag in hoeverre moet worden uitgesplitst welke VoIP applicaties wel en welke applicaties niet worden geblokkeerd. Het is waarschijnlijk dat een ISP die volgens aanpak a) in het mobiele netwerk VoIP blokkeert daarbij tenminste de populaire en daarmee bekende VoIP applicaties meeneemt. Een beperkte opsomming van een aantal bekende applicaties is dan voor de brede groep gebruikers voldoende om zich een oordeel te vormen. De ISP zal deze applicaties hoogst waarschijnlijk kennen omdat hij er specifiek op filtert, in het hier gegeven voorbeeld door te detecteren op de combinatie van bepaalde IP adressen en het SIP protocol. In optie b) van deze use case waarbij de blokkering uitgaat van de applicatie op de mobiele terminal kan dit mechanisme zelf worden uitgelegd, met een verwijzing naar de applicatie store voor informatie per applicatie en een aantal voorbeelden van bekende applicaties die geraakt worden.
- *Welk effect?* Het effect van het traffic management maatregel is duidelijk: de VoIP applicaties werken niet over mobiele netwerken.

- *Wanneer?* Ook in deze use case is de “wanneer” vraag eenvoudig te beantwoorden: altijd.

Tijdkritische applicaties voorrang geven bij congestie

- *Welke applicaties en diensten?* Bij selectie van real-time verkeer op basis van protocol is het goed mogelijk om door het noemen van aantal bekende klassen van toepassingen gekoppeld aan deze protocollen, zoals webbrowsing, internettelefonie, videoconferencing en streaming video, een brede groep eindgebruikers een goede indruk te geven van de applicaties die profiteren van de traffic management maatregel. Het ligt voor de hand om ook de namen van een aantal bekende applicaties voor deze toepassingen te noemen. Een precies overzicht van de applicaties die profiteren is niet te maken, omdat ISPs en andere partijen geen compleet zicht hebben op de applicaties die van gegeven protocollen, zoals http en rtp, gebruik maken.
- *Welk effect?* Het effect van de traffic management maatregel is in kwalitatieve zin goed uit te leggen: de eindgebruiker krijgt bij de betrokken toepassingen waarschijnlijk een betere dienstervaring dan in het geval dat er tijdens congestie geen maatregelen zouden worden genomen. Andere toepassingen, zoals e-mail, zullen langzamer worden. Deze vertraging is in het algemeen niet merkbaar voor de meeste eindgebruikers.
- *Wanneer?* De “wanneer?” vraag is in deze use case lastiger te beantwoorden. Aannemende dat congestie een bijzondere omstandigheid in het netwerk is die niet op vaste tijden voorkomt, is het noemen van tijdstippen niet mogelijk. Voor eindgebruikers is het wel nuttig om te weten onder welke omstandigheden er sprake kan zijn van congestie, bijvoorbeeld lokaal in het mobiele netwerk bij evenementen. Een verdere detaillering lijkt lastig. Het totaal van de begrijpelijke informatie is desondanks nog steeds nuttig voor de eindgebruiker, omdat hij wel in grote lijnen op de hoogte is van hoe de applicaties die hij zelf belangrijk vindt, behandeld worden tijdens congestie.

3.4.2 Geen verplichting voor begrijpelijke informatie

Zoals eerder beschreven in paragraaf 3.2.2 zijn meerdere partijen in een positie om een vertaling te maken van technische naar voor de eindgebruikers begrijpelijke informatie: de ISPs zelf, maar ook technische experts uit de Internet community, vergelijkingssites, consumentenorganisaties en anderen. Van deze partijen zouden alleen de ISPs vanuit het wetsvoorstel Telecommunicatiewet verplicht kunnen worden om begrijpelijke informatie te publiceren. Het voorstel in dit onderzoek is om ISPs hier niet toe te verplichten. Hiervoor bestaat een aantal redenen:

- Doordat de begrijpelijke informatie naar zijn aard ontstaat uit een deels subjectieve vertaling vanuit de technische informatie is het lastig om duidelijke verplichtingen over de inhoud van de begrijpelijke informatie op te leggen. Dit blijkt ook al uit de voorbeelden uit de vorige paragraaf. Een dergelijke verplichting zou ook lastig te handhaven zijn omdat er geen objectieve toets beschikbaar is om de verschafte informatie te beoordelen.
- Een verplichting voor ISPs lijkt daarnaast niet nodig. ISPs zullen zelf al geneigd zijn om de technische informatie, die ze wel verplicht op een goed zichtbare plaats moeten publiceren, aan hun (potentiële) klanten toe te lichten door een vertaling naar begrijpelijke informatie te maken. Tijdens de workshops en in nagekomen reacties heeft een aantal ISPs verklaard inderdaad om deze reden begrijpelijke informatie te gaan publiceren.
- Naast het uitleggen van de effecten van traffic management maatregelen voor de eindgebruiker zullen ISPs ook willen uitleggen waarom ze dergelijke maatregelen nemen. Traffic management maatregelen staan tot nu toe in een zeker kwaad daglicht doordat de afgelopen jaren vooral incidenten in de publiciteit zijn gekomen waaruit negatieve gevolgen voor eindgebruikers bleken. Voor ISPs is dit een stimulans om uit te leggen

waarom ze bepaalde maatregelen nemen en hoe ze daarbij de afweging maken tussen de belangen van eindgebruikers, content aanbieders en hun eigen belangen.

Een argument voor een verplichting aan ISPs om begrijpelijke informatie te publiceren is dat daarmee ook een zekere vergelijkbaarheid tussen begrijpelijke informatie van verschillende ISPs kan worden bereikt. Doordat het lastig is om objectieve eisen te formuleren voor de inhoud van de informatie zou het echter moeilijk zijn om dit mechanisme in de praktijk goed te laten werken. In het hier voorgestelde model kan vergelijkbaarheid op andere manieren ontstaan. Zo kunnen vergelijkingssites de door hen geselecteerde en geïnterpreteerde elementen van traffic management maatregelen opnemen in hun overzichten van de door verschillende ISPs aangeboden internettoegangsdiensten. De auteurs van fora en blogs kunnen de traffic management maatregelen die zij belangrijk vinden becommentariëren en de vergelijking maken tussen verschillende ISPs. Via deze routes ontstaat vergelijkbaarheid op een door marktpartijen en belanghebbenden gestuurde manier. Er ontstaat waarschijnlijk geen breed, door alle partijen gebruikte aanpak of formaat. Verschillende vergelijkingssites, fora en bloggers zullen zich voor wat betreft de inhoud en de presentatie van hun begrijpelijke informatie richten op de aspecten die voor hun doelgroep het meest relevant zijn.

4 Conclusie

De analyse in dit rapport richt zich op twee belangrijke elementen die nodig zijn voor het uitwerken van de transparantieverplichting in (lagere) regelgeving. Als eerste is de reikwijdte van de te definiëren verplichting van belang. De reikwijdte hangt nauw samen met de uitgangspunten die voor de transparantie worden gehanteerd en bepaalt in welke situaties aanbieders informatie moeten verschaffen over traffic management maatregelen. Ten tweede is de omschrijving van de typen informatie die transparant moeten worden van belang, inclusief de mate van detail daarin.

4.1 Uitgangspunten en reikwijdte voor transparantie

Vanuit het wetsvoorstel Telecommunicatiewet kan een transparantieverplichting worden opgelegd aan aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten. In de praktijk zal een dergelijke verplichting gaan gelden voor ISPs. De reikwijdte van de verplichting wordt bepaald door een afbakening op vijf punten. In dit rapport wordt voorgesteld dat een transparantieverplichting aan de orde is:

1. Voor die traffic management maatregelen waarover de aanbieder *controle* of *zeggenschap* heeft.
   Hierbij kunnen traffic management maatregelen waarover de aanbieder *zeggenschap* heeft buiten de netwerken vallen waarover de aanbieder complete *controle* heeft.
2. Voor aanbieders van *vaste* netwerken en diensten en voor aanbieders van *mobiele* netwerken en diensten.
3. Voor aanbieders die zich richten op *particuliere* eindgebruikers en voor aanbieders die zich richten op *zakelijke* eindgebruikers.
   Een kanttekening hierbij is dat de praktische uitwerking van de transparantieverplichting in de grootzakelijke markt in een aantal situaties deels via de met eindgebruikers afgesloten SLAs kan lopen.
4. Voor traffic management maatregelen die aanbieders nemen in de *internettoegangsdienst* èn voor het effect dat de door hen geleverde *managed services* hebben op de internettoegangsdienst als geheel.
   Het opnemen van het effect van managed services op de internettoegangsdienst is een uitbreiding van de reikwijdte ten opzicht van traditionele analyses waarin alleen het effect van maatregelen toegepast op verkeerstromen binnen de internettoegangsdienst wordt meegenomen. Deze uitbreiding is van belang vanuit de verwachting dat managed services in de toekomst in aantal en belang zullen groeien en het effect dat de managed services kunnen hebben op de eveneens belangrijke internettoegangsdienst.
5. Binnen de internettoegangsdienst voor traffic management maatregelen die leiden tot het *verschillend behandelen van verkeerstromen*.

4.2 Transparant te maken informatie, betrokken partijen en processen

De informatie over traffic management maatregelen die vanuit de transparantieverplichting beschikbaar komt, moet leiden tot de gewenste sturende werking richting ISPs. Dit effect is het hoofddoel van de transparantieverplichting. Daarnaast moeten de informatie en de processen eromheen voldoen aan aantal bijkomende criteria zoals goede handhaafbaarheid, toekomstvastheid, vergelijkbaarheid, toegankelijkheid, beperkte kosten voor de betrokken marktpartijen, waarborgen voor netwerkintegriteit en correcte omgang met de

concurrentiegevoeligheid van informatie. Dit laat zien dat de vorm en inhoud van de informatie in nauwe samenhang met de betrokken partijen en de processen waarin ze een rol spelen moet worden beschouwd. Het voorstel in dit onderzoek is om bij het inrichten van de transparantieverplichting onderscheid te maken tussen twee soorten informatie: technische en begrijpelijke informatie.

- De *technische informatie* beschrijft in technische termen de traffic management maatregelen die een ISP instelt. Deze informatie biedt met name voor experts een duidelijke toegang tot de feitelijke technische maatregelen. Hierbij gaat het om de antwoorden op drie vragen:
  – Welke verkeerstroom wordt door traffic management maatregelen speciaal behandeld?
  – Welke maatregel wordt toegepast op deze verkeerstroom?
  – Wanneer wordt deze maatregel toegepast?

  ISPs zijn in verreweg de beste positie om technische informatie te verschaffen over de traffic management maatregelen die zij nemen. Gezien het belang van de technische informatie voor de handhaving èn voor het opstellen van begrijpelijke informatie, is het voorstel om ISPs te verplichten de technische informatie te verschaffen over hun traffic management maatregelen, voor zover ze binnen de hierboven beschreven reikwijdte vallen. De mate van detail in de informatie die de ISPs moeten opleveren volgt uit een afweging tussen de eerder genoemde criteria. Daaruit volgt bijvoorbeeld dat de technische omschrijving van het “welke verkeerstroom” deel van de technische informatie tenminste moet ingaan op de (klassen van) toepassingen inclusief de opsomming van de (combinaties van) technische parameters die het verkeer karakteriseren. Meer gedetailleerde informatie hoeft niet publiek beschikbaar te worden gemaakt maar kan wel waardevolle rol spelen in de handhaving van de transparantieverplichting. Hierbij is goed voorstelbaar dat een ISP in het kader van een specifieke handhavingsactie de gedetailleerdere informatie binnen een vertrouwelijke context aan de toezichthoudende instantie ter beschikking stelt.

- De *begrijpelijke informatie* beschrijft de gevolgen van de traffic management maatregelen voor de eindgebruikers, in termen die een brede groep eindgebruikers begrijpt. Hierbij gaat het om:
  – Welke applicaties en diensten een speciale behandeling krijgen.
  – Wat het effect van de speciale behandeling is of kan zijn op de beleving van de dienst door de eindgebruiker.
  – Wanneer dit effect merkbaar is.

  De voor de gemiddelde eindgebruiker begrijpelijke informatie ontstaat door vertaling van de technische informatie naar de belevingswereld van de eindgebruiker. Op hoofdlijnen is deze vertaling relatief eenvoudig. Tegelijkertijd is de vertaling vaak subjectief, doordat er naast de traffic management maatregelen andere factoren van invloed zijn op de dienstbeleving van de eindgebruiker.

  In dit onderzoek wordt voorgesteld om geen verplichting in te voeren voor het beschikbaar maken van begrijpelijke informatie. De verwachting is dat ISPs uit zichzelf al een vertaling naar begrijpelijke informatie zullen maken om de technische informatie, die ze wel verplicht op een goed zichtbare plaats moeten publiceren, aan hun (potentiële) klanten toe te lichten. Daarnaast is het in veel gevallen lastig om een eenduidige verplichting te formuleren voor de subjectieve vertaling en de interpretaties die nodig zijn bij het opstellen van begrijpelijke informatie.

Als de gevraagde technische informatie beschikbaar is, zijn naast de ISPs ook andere partijen in staat om de vertaling te maken van technische naar voor de eindgebruikers begrijpelijke informatie. Dat zijn bijvoorbeeld technische experts uit de Internet community, vergelijkingssites en content providers. De begrijpelijke informatie ontstaat via deze routes op een door marktpartijen en belanghebbenden gestuurde manier. Verschillende vergelijkingssites, fora en bloggers zullen zich voor wat betreft de inhoud en de presentatie van hun begrijpelijke informatie richten op de aspecten die voor hun doelgroep het meest relevant zijn. Partijen die zich benadeeld voelen door gepubliceerde informatie kunnen een beroep doen op de bestaande civielrechtelijke middelen zoals de Wet Oneerlijke Handelspraktijken.

5 Referenties

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

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

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

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

[7] Richtlijn 2009/140/EG, 25 november 2009, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:NL:PDF

[8] Richtlijn 2009/136/EG, 25 november 2009, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:NL:PDF

[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, 30 June 2010, http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/net_neutrality/nn_questionnaire.pdf

[10] Wetsvoorstel Telecommunicatiewet, consultatieversie dd 15 april 2010, http://www.internetconsultatie.nl/nrfimplementatie/document/122

[11] Wetswijziging voor vrij toegankelijk internet, nieuwsbericht ministerie EL&I, 03 november 2010, http://www.rijksoverheid.nl/ministeries/eleni/nieuws/2010/11/03/wetswijziging-voor-vrij-toegankelijk-internet.html

[12] Netwerkneutraliteit: stand van zaken in Nederland, Dialogic, 10 juni 2009, http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2009/10/13/netwerkneutraliteit-stand-van-zaken-in-nederland.html

[13] Network Neutrality and Transparency, Theory, Experimental Research, Policy Conclusions, TILEC, August 2010, http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2010/09/01/network-neutrality-and-transparency.html

[14] Tweede Kamer motie Aasted Madsen-van Stiphout-Vos, 27 879, nr. 30 http://www.rijksbegroting.nl/algemeen/gerefereerd/1/4/5/kst145334.html

[15] YouTube, http://www.youtube.com

[16] Uitzending Gemist, http://www.uitzendinggemist.nl

[17] German Carrier T-Mobile Blocking Skype, mocoNews.net, April 1, 2009, http://moconews.net/article/419-german-carrier-t-mobile-blocking-skype/

[18] Vodafone to keep VoIP out of the 3G network, ZDNet UK, 27 July, 2005, http://www.zdnet.co.uk/news/mobile-working/2005/07/27/vodafone-to-keep-voip-out-of-the-3g-network-39210642/

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

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

[21] Rogers Network Management Policy, 25 oktober 2010 op http://www.rogers.com/web/content/network_management

[22] Bell: Network management, 25 oktober 2010 op http://internet.bell.ca/index.cfm?language=en&method=content.view&content_id=12119

[23] BEREC Response to the European Commission's consultation on the open Internet and net neutrality in Europe, BoR (10) 42, 30 September 2010, http://www.erg.eu.int/doc/berec/bor_10_42.pdf

[24] FCC, In the Matter of Preserving the Open Internet, Broadband Industry Practices, GN Docket No. 09-191, WC Docket No. 07-52, October 22, 2009, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-93A1.doc

[25] 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

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

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

[28] Regeling universele dienstverlening en eindgebruikersbelangen, te vinden via www.overheid.nl

A Passages uit relevante wet- en regelgeving

Hieronder worden een aantal relevante passages aangehaald uit de nieuwe Europese universeledienstrichtlijn [8] en het Nederlandse Wetsvoorstel Telecommunicatiewet [10].

A.1 Europese Universeledienstrichtlijn

Artikel 20(1)(b)

De lidstaten zorgen ervoor dat de consumenten en andere hierom verzoekende eindgebruikers die zich abonneren op diensten waarbij een aansluiting tot het openbare communicatienetwerk en/of openbare elektronischecommunicatiediensten worden aangeboden, recht hebben op een contract met een onderneming of ondernemingen die dergelijke aansluiting en/of diensten aanbieden. In het contract worden ten minste de volgende elementen in een heldere, begrijpelijke en gemakkelijk toegankelijke vorm gespecificeerd:

….

b) de verstrekte diensten, met name:

…

- *informatie over eventuele beperkingen inzake toegang tot en/of gebruik van diensten en toepassingen, indien zulks volgens de nationale wetgeving overeenkomstig de Gemeenschapswetgeving toegestaan is;*

…

- *door de onderneming ingestelde procedures om het verkeer te meten en te sturen, om te voorkomen dat een netwerkaansluiting tot haar maximum wordt gevuld of overloopt, en over de wijze waarop deze procedures gevolgen kunnen hebben voor de kwaliteit van de dienstverlening;*

…

- *alle beperkingen die de leverancier heeft opgelegd met betrekking tot het gebruik van geleverde eindapparatuur;*

Artikel 21(3)(c) en (d)

De lidstaten zorgen ervoor dat de nationale regelgevende instanties de aanbieders van openbare elektronischecommunicatienetwerken en/of openbare elektronischecommunicatiediensten kunnen verplichten om, onder andere:

…

c) abonnees te informeren over eventuele wijzigingen in de voorwaarden voor beperking van de toegang tot en/of het gebruik van diensten en toepassingen, indien zulks volgens de nationale wetgeving overeenkomstig de Gemeenschapswetgeving toegestaan is;

d) informatie te verstrekken over door de aanbieder ingestelde procedures om het verkeer te meten en vorm te geven, om te voorkomen dat een netwerkaansluiting vol- of overloopt, en over de wijze waarop deze procedures gevolgen kunnen hebben voor de kwaliteit van de dienstverlening;

A.2 Wetsvoorstel Telecommunicatiewet

Artikel 7.3

1. Bij ministeriële regeling kan worden bepaald dat aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten transparante, vergelijkbare, toereikende, actuele, duidelijke en volledige informatie bekendmaken over:

…

d. eventuele beperkingen van de toegang tot of het gebruik van diensten en toepassingen.

2. De informatie, bedoeld in het eerste lid, wordt bekendgemaakt in een gemakkelijk toegankelijke vorm. Bij ministeriële regeling kunnen regels worden gesteld ten aanzien van de vorm waarin de informatie bekend wordt gemaakt.

…

4. Bij ministeriële regeling kunnen regels worden gesteld over het door de aanbieder van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten aan de eindgebruiker en Onze Minister te verstrekken informatie met betrekking tot:

…

b. wijzigingen in de voorwaarden voor beperking van de toegang tot of het gebruik van diensten en toepassingen;

c. de door de aanbieder ingestelde maatregelen bij congestie en de gevolgen daarvan voor de kwaliteit van de dienstverlening;

…

Memorie van toelichting bij artikel 7.1

In artikel 7.1, eerste lid, onder b, van de wet is reeds geregeld dat de te verstrekken diensten in het contract moet worden opgenomen. De volgende onderwerpen worden bij of krachtens algemene maatregel verder uitgewerkt en zijn in feite een uitwerking van welke diensten door de aanbieder worden verstrekt:

…

- een ander onderwerp dat bij of krachtens algemene maatregel van bestuur zal worden uitgewerkt is het informeren van de eindgebruiker over de eventuele beperkingen die de aanbieders aanbrengt met betrekking tot de toegang of het gebruik van diensten. Dit houdt onder andere in dat telecomoperators eventuele gebruiksbeperkingen transparanter moeten maken, waardoor het bijvoorbeeld duidelijk is welk toestel de beste mogelijkheden biedt om Skype te gebruiken;

….

- het informeren van de consument over de wijze waarop de aanbieder het netwerkverkeer meet en stuurt, teneinde te voorkomen dat een netwerkaansluiting overloopt. Ook moet daarbij door de aanbieder worden aangegeven welke gevolgen deze maatregelen kunnen hebben voor de kwaliteit van de dienstverlening;

…

- alle beperkingen die de leverancier heeft opgelegd met betrekking tot het gebruik van geleverde eindapparatuur.

B Deelnemers aan workshops

De uitgangspunten voor transparantie en het voorstel voor het transparantiemodel zijn met een aantal marktpartijen en belangenorganisaties besproken in twee interactieve workshops. Onderstaande personen hebben aan één of beide workshops deelgenomen.

Niels van Veen	BCPA
Ben Woldring	Bencom
Daphne van der Kroft	Bits of Freedom
Ot van Dalen	Bits of Freedom
Arnoud Vermeer	Bits of Freedom
Feyo Sickinghe	BOT
Olaf Olmer	BT
Hans van der Giessen	Caiway
Maurice Wessling	Consumentenbond
Jeroen Schouten	Google
Ad Bresser	KPN
Paul Knol	KPN
Hans Bakhuizen	NPO
Egon Verharen	NPO
Peter-Paul de Goeij	Online
Paul Brackel	OMI2
Stef de Vries	OPTA
Nadine van Herten	RTL
John de Jong	RTL
Roderick van Houten	T-Mobile
Edwin Evenhuis	UPC
Roger Schobben	UPC
Michiel Prinsen Geerligs	Vodafone
Walter Kroeze	Vodafone
Dirk Segers	Vodafone
Machiel Bolhuis	Ziggo