Nummeridentificatie en de bescherming van persoonsgegevens

een gemotiveerde terugkoppeling
op de CBP-consultatie van november 2003

Een CBP-document
oktober 2004

INHOUDSOPGAVE

1. Managementsamenvatting

Algemeen
In de consultatie over nummeridentificatie heeft het CBP zich laten informeren over zienswijzen en uitvoeringsaspecten aangaande de verwerking van persoonsgegevens in het kader van deze dienst. Daarbij is alleen aandacht besteed aan de variant van nummeridentificatie waarbij het nummer van de beller wordt doorgegeven aan de gebelde partij.

Het eerste gedeelte van de consultatie ging over de toepassing van enige bepalingen uit artikel 11.9 uit de Telecommunicatiewet (Tw) betreffende de verwerking van persoonsgegevens in het kader van nummeridentificatie en, indien die bepalingen niet van toepassing zijn, de werking van de Wet bescherming persoonsgegevens (WBP).
Achtereenvolgende onderwerpen betroffen ISDN, SMS en internettelefonie (Voice over IP) en overige internetdiensten, waaronder e-mail.
Vervolgens kwamen in de consultatie situaties aan de orde waarin netwerk en telefoondienst niet in één hand zijn. Daarbij zijn vragen gesteld over de verantwoordelijkheid voor het verstrekken van het nummer, de grondslag daarvoor en over het realiseren van blokkeringen.
Het derde gedeelte had betrekking op de informatieverplichtingen uit hoofde van Tw en/of WBP. Duidelijk moet zijn op wie de informatieverplichtingen rusten, en welke eisen het CBP stelt aan de te verstrekken informatie voor wat betreft de beschikbaarheid, de toegankelijkheid en de volledigheid ervan, ook waar het gaat over de relatie tussen nummeridentificatie en geheime telefoonnummers.
Ten slotte kwamen situaties aan de orde waarin men geen reëel gebruik blijkt te kunnen maken van de geboden blokkeringsmogelijkheden.

Reikwijdte van artikel 11.9 Tw in relatie met WBP
Vraag 1: ISDN
Een ISDN-aansluiting kan bestaan uit twee lijnen met vier bijbehorende MSN-nummers, maar het kunnen ook honderden lijnen zijn met duizenden nummers. Het is de vraag of de verstrekking van elk van die nummers kan worden aangemerkt als nummeridentificatie. Vervolgens moet worden bepaald welke blokkeringsmogelijkheden dienen te worden aangeboden volgens de Tw, en bij niet toepasselijkheid daarvan volgens de WBP.

Volgens het CBP kan de verstrekking van elk van de bij een ISDN-aansluiting behorende nummers worden aangemerkt als nummeridentificatie. Artikel 11.9 Tw is daarop van toepassing. Wat de blokkeringsmogelijkheden betreft levert het per gesprek blokkeren door de gebruiker geen problemen op. Het recht van de abonnee om voor elke afzonderlijke abonneelijn de verstrekking te blokkeren moet zo worden uitgelegd dat de abonnee ten minste het recht heeft om alle nummers behorend bij het netwerkaansluitpunt tegelijk te blokkeren.
Of de abonnee ook het recht heeft om voor elk afzonderlijk nummer een blokkering te verlangen moet worden uitgemaakt door OPTA dan wel de rechter. Aanbieders zouden deze optie aan willen bieden, maar zij geven aan dat er hierbij technische en economische grenzen zijn.
Het CBP sluit zich verder aan bij de opvatting van de sector dat de abonnee niet het recht heeft zelf te bepalen welke van de bij een ISDN-aansluiting behorende nummers in het kader van nummeridentificatie worden verstrekt.

Vragen 2 en 3: SMS
Bij nummeridentificatie wordt het nummer van de beller aan het gebelde aansluitpunt verstrekt via het signaleringskanaal. Een signalering kan evenwel meer informatie bevatten dan alleen het bellende telefoonnummer, er is ruimte voor aanvullende tekst. Van die ruimte maakt een SMS-bericht gebruik. Bij een SMS-bericht komt dus tegelijk met het nummer ook het bericht binnen.

Ook hier is het de vraag in hoeverre de regeling van artikel 11.9 Tw van toepassing is. Als dit artikel op SMS-berichten ziet, is het de vraag of de daarin voorgeschreven blokkeringsmogelijkheden technisch kunnen worden gerealiseerd.

Omdat er bij SMS-diensten geen nummers worden verstrekt voordat de verbinding tot stand komt, is er geen sprake van nummeridentificatie. Hiermee blijft artikel 11.9 Tw buiten werking. Op de verstrekking van nummers in het kader van SMS is derhalve de WBP van toepassing. Het meezenden van het oproepende nummer bij SMS-berichten is veelal aan te merken als een verstrekking van een persoonsgegeven. De grondslag voor die verwerking kan worden gevonden in artikel 8, onder a, b of f WBP.
Uit de respons zou men kunnen afleiden dat het technisch mogelijk is SMS-berichten af te leveren bij de geadresseerde zonder vermelding van het oproepende nummer. In dat geval is er geen sprake van noodzakelijkheid voor de uitvoering van de overeengekomen SMS-dienst en kan derhalve voor de verstrekking geen grondslag worden gevonden in artikel 8, onder b WBP. Voor e-mail daarentegen wel, omdat e-mail niet kan worden afgeleverd zonder het IP-adres van de verzender. Voor SMS resteert derhalve de grondslag van artikel 8, onder a WBP (toestemming) dan wel die onder f (gerechtvaardigd belang). De aanbieder zal dus expliciet om toestemming dienen te vragen of afdoende waarborgen moeten stellen, bijvoorbeeld via het aanbieden van blokkeringsfaciliteiten en het verstrekken van informatie.

Vraag 4: Internettelefonie en overige internetdiensten
Het is voorts de vraag in hoeverre de bepalingen voor nummeridentificatie gelden voor internettelefonie. De vele gedaantes die deze vorm van telefonie kent variëren ruwweg van zuivere internettoepassingen waarbij een ISP alleen maar toegang hoeft te bieden en verder niets bijzonders hoeft te doen om het telefoneren mogelijk te maken tot allerhande vormen waarbij aanbieders van traditionele telefonie een rol spelen.

Het CBP doet geen uitspraak over de toepasselijkheid van de Tw op internettelefonie, maar geeft een overzicht van criteria die een rol spelen bij de beoordeling of artikel 11.9 Tw erop van toepassing is. Als een concrete variant voorligt ter beoordeling zal het CBP over de toepassing van die criteria overleggen met OPTA. Op internetdiensten waarbij het nummer tegelijk met het bericht wordt verstrekt is niet artikel 11.9 Tw van toepassing maar de WBP.

Verantwoordelijkheden als netwerk en communicatiedienst dan wel nummeridentificatie niet in één hand zijn
Vragen 5 en 6: toedeling verantwoordelijkheden
In twee situaties is niet duidelijk wie moet worden aangemerkt als de aanbieder van nummeridentificatie dan wel de verantwoordelijke voor het verstrekken van het nummer. Soms beschikt een aanbieder van vaste of mobiele telefonie niet over een eigen netwerk. De tweede situatie is die van carrier select, waarbij de abonnee zowel contracteert met een telefonieaanbieder als met de aanbieder van carrier select. Duidelijk moet zijn op wie de verplichtingen van artikel 11.9 Tw dan wel de WBP rusten.

Het CBP acht de aanbieder van de telefoondienst verantwoordelijk voor het aanbieden van nummeridentificatie en het verstrekken van het nummer. De netwerkaanbieder is de bewerker in de zin van de WBP. De eindgebruiker kan de aanbieder van de dienst met wie hij heeft gecontracteerd aanspreken op diens verplichtingen uit hoofde van artikel 11.9 Tw.
Als een eindgebruiker gebruik maakt van carrier select, zullen gesprekken de ene keer door de telefonieaanbieder worden afgehandeld, de andere keer door de carrier select aanbieder. Ieder van de dienstverleners is verantwoordelijk voor het deel van de gesprekken dat hij afhandelt.

Vraag 7: aanvragen van een lijnblokkering
De sector werd gevraagd wie een lijnblokkeringsmogelijkheid dient aan te bieden: de netwerkaanbieder, de telefonieaanbieder dan wel de aanbieder van carrier select.

Het CBP vindt dat niet de netwerkaanbieder, maar de dienstenaanbieder een mogelijkheid tot lijnblokkering dient aan te bieden. Als daarvoor een centraal punt wordt ingericht is dat prima.

Vraag 8: bevoegdheid tot verstrekking van nummers aan derden
Er zijn dienstenaanbieders die de netwerkaanbieder verantwoordelijk houden voor de inrichting van nummeridentificatie.

Volgens het CBP kan de aanbieder van een netwerk niet zelf besluiten tot verstrekking van nummers in het kader van nummeridentificatie, maar dient deze de dienstaanbieder te volgen. Niettemin kan in bepaalde gevallen een zelfstandige bevoegdheid tot verstrekking voor de netwerkaanbieder bestaan, in het bijzonder in situaties waarin een wettelijke verplichting bestaat, zoals die waarbij de netwerkaanbieder verplicht is het oproepende nummer te verstrekken aan alarmcentrales. In dat geval is de grondslag van artikel 8, onder c WBP van toepassing.
De bevoegdheid tot verstrekking van persoonsgegevens door de dienstaanbieder dient te worden bepaald op grond van de WBP. Van een wettelijke verplichting tot verstrekking in de zin van artikel 8, onder c WBP is geen sprake. Het nalaten van een blokkering kan niet worden opgevat als toestemming in de zin van artikel 8, onder a WBP. Ook het aangaan van een overeenkomst van telefonie impliceert geen toestemming tot het verstrekken van nummers in het kader van nummeridentificatie. Nummeridentificatie moet worden gezien als een aparte faciliteit die geen onlosmakelijk onderdeel vormt van de dienst.
In de regel kan de dienstaanbieder voor verstrekking een grondslag vinden in artikel 8, onder b dan wel onder f WBP.

Volledigheidshalve merkt het CBP naar aanleiding van opmerkingen uit de sector op dat de eindgebruiker niet als de verantwoordelijke voor de verstrekking kan worden aangemerkt.

Vraag 9: doorschakelen
Bij doorschakelen is niet helder hoe nummeridentificatie precies werkt en daarmee niet wie als verantwoordelijke voor verstrekkingen kan worden aangemerkt of wat de grondslag voor verstrekking is. Als ik iemand bel, die zijn toestel heeft doorgeschakeld naar zijn mobiele toestel is het de vraag of nu mijn nummer wordt doorgegeven dan wel het gebelde nummer.
Dit blijkt niet te zijn gestandaardiseerd. Het CBP vindt het een goed uitgangspunt om de originerende partij waarop het oproepende aansluitpunt is aangesloten verantwoordelijk te laten zijn voor het realiseren van de keuzes van de oproepende gebruiker. Wat het informeren van het publiek betreft dient de dienstaanbieder zijn oproepende abonnees te informeren over welk nummer nu precies wordt verstrekt en hoe de oproepende abonnee dat zou kunnen verhinderen.

Informatieverplichtingen
Alvorens in te gaan op een aantal specifieke vragen geeft het CBP gemotiveerd aan dat de informatieverplichtingen niet uitputtend zijn geregeld in de Tw en de daarop gebaseerde uitvoeringsregelingen: ook uit de WBP kunnen informatieverplichtingen worden afgeleid.

Vraag 10: verantwoordelijkheid voor het beschikbaar stellen van informatie bij gebruik netwerk van derden
Aanbieders van carrierdiensten en ook sommige mobiele aanbieders zonder eigen netwerk, bieden zelf geen informatie aan maar verwijzen naar de netwerkaanbieder.

De dienstaanbieder, en dus ook de aanbieder van carrierdiensten, is tevens de verantwoordelijke voor de gegevensverstrekking in de zin van de WBP, dus op hem rusten de informatieverplichtingen uit hoofde van de wet. De netwerkaanbieder heeft slechts verplichtingen jegens de dienstaanbieder.

Vraag 11: toegankelijkheid en beschikbaarheid informatie
Het CBP is het niet met de sector eens dat de voorhanden zijnde informatie in alle opzichten voldoet aan de gestelde eisen van beschikbaarheid en toegankelijkheid. Beoordeling kan echter slechts per geval. Wel worden vuistregels gegeven.

Vraag 12: volledigheid van de beschikbare informatie
Het CBP heeft geconstateerd dat over een aantal onderwerpen geen informatie voorhanden is. Het gaat vooral om informatie over het terzijde stellen van blokkeringen bij oproepen naar alarmcentrales en het traceren van daders van telefoonhinder. In het consultatiedocument zijn ook doorschakelscenario's en defaultinstellingen bij geheime telefoonnummers aan de orde gesteld.
De sector meent bij het informeren niet verder te hoeven gaan dan waartoe de Tw verplicht. Ook wordt door de sector opgemerkt dat de Tw alleen verplicht tot het beschikbaar te stellen van algemene informatie over de werking van nummeridentificatie en de blokkeringen, en niet over uitzonderingssituaties zoals de genoemde.

Het CBP is een andere opvatting toegedaan. Als de Tw al niet verplicht tot het verstrekken van specifieke informatie over de genoemde onderwerpen, kan artikel 33 WBP met zich meebrengen dat nadere informatie is vereist in de genoemde gevallen om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

Vraag 13: default bij geheime nummers
Aanbieders zetten nummeridentificatie standaard aan, ook als de abonnee een geheim nummer heeft. Zonder enige handeling van de beller zal een geheim nummer automatisch worden verstrekt aan derden.
Het CBP ziet geen basis in de wet om de dienst nummeridentificatie in het geval van een abonnee met een geheim nummer standaard uit te zetten. Gelet op de aard van een geheim nummer en de diverse belangen van abonnees bij het nemen daarvan, geldt hier op grond van artikel 33 WBP een verplichting om de abonnee met een geheim nummer nader te informeren over de default-instelling van de dienst nummeridentificatie. Bij het ontbreken van iedere informatie kan niet meer worden gesproken van een eerlijke en zorgvuldige verwerking in de zin van artikel 6 WBP.

Effectiviteit blokkeringen
Vragen 14 en 15: geen reële blokkeringsmogelijkheden
In een aantal gevallen blijkt de gebruiker geen reëel gebruik te kunnen maken van de aangeboden blokkeringsmogelijkheden. Sommige diensten zijn niet toegankelijk wanneer gebruik is gemaakt van een blokkeringsmogelijkheid. Soms blijken ISP's toch het oproepende nummer te ontvangen, ook als de doorgifte ervan is geblokkeerd.

Bij het inbellen naar een ISP teneinde een andere telecommunicatiedienst af te nemen, kan het netwerkaansluitpunt van de ISP niet worden beschouwd als het opgeroepen netwerkaansluitpunt. Het CBP kan zich daarom vinden in de opvatting dat een ISP zich niet steeds als eindgebruiker hoeft op te stellen. In dat geval zijn de regels van artikel 11.9 Tw niet van toepassing. Als daarentegen naar een aanbieder wordt gebeld om een andere dienst dan een telecommunicatiedienst af te nemen (te denken valt aan programma's voor elektronische spaardiensten waarbij de identificatie van de spaarder verloopt via nummeridentificatie) geldt artikel 11.9 Tw wél en dienen de gekozen blokkeringen te worden gerespecteerd. Over de toepasselijkheid van artikel 11.9 Tw bij toegevoegdewaardediensten (deels telecommunicatie, deels anders) zal per geval moeten worden geoordeeld. Het CBP zal zich in dat geval conformeren aan het oordeel van OPTA.
Of een ISP uit nummeridentificatie verkregen nummers mag vastleggen voor facturering en dergelijke moet worden beoordeeld op basis van artikel 11.5 Tw. Een noodzaak daartoe is niet steeds aanwezig.

De toezichtsvraag
Het CBP ziet toe op de verwerking van persoonsgegevens in het algemeen, waaronder de verwerkingen door telecommunicatieaanbieders. Het toezicht op de naleving van de Telecommunicatiewet, waaronder het hoofdstuk over de bescherming van persoonsgegevens en de persoonlijke levenssfeer, is opgedragen aan OPTA. Waar bevoegdheden elkaar overlappen dienen CBP en OPTA hun rolverdeling onderling af te stemmen. Voor nummeridentificatie ziet het CBP in elk geval een taak voor zich weggelegd met betrekking tot regels over het verstrekken van gegevens, het blokkeren daarvan en het informeren van de betrokkenen daarover.

Overige
Gelet op de respons moeten de ontvangen reacties als representatief voor de sector worden beschouwd. Zie verder Bijlage 1, waar ook overige niet-inhoudelijke aspecten aan de orde komen.

2. Achtergrond van de consultatie

2.1. Algemeen

Het College bescherming persoonsgegevens (CBP) heeft op 19 november 2003 partijen uit de telecommunicatiesector uitgenodigd om te reageren op het door het CBP voorbereide consultatiedocument over het thema Nummeridentificatie. Daarbij heeft het een gemotiveerde terugkoppeling toegezegd. Dit document bevat die terugkoppeling.

2.2. Kader van de consultatie

Het CBP wil meer aandacht geven aan voorlichting over de bescherming van persoonsgegevens bij telecommunicatie. Voorlichting die gebaseerd is op een uitgewerkt normenstelsel. Omdat de complexiteit van de wet- en regelgeving in relatie tot de telecommunicatiepraktijk verhindert dat alle onderwerpen die verband houden met de bescherming van persoonsgegevens in de telecommunicatiesector in één keer behandeld kunnen worden, hanteert het CBP hierbij een themagewijze aanpak.

2.3. De consultatie over nummeridentificatie

De consultatie van 19 november 2003 (kenmerk z2003-0091) had Nummeridentificatie als thema. Op verwerkingen van persoonsgegevens in het kader van nummeridentificatie zijn zowel de regels van de Wet bescherming persoonsgegevens (WBP) van toepassing als die van de Telecommunicatiewet (Tw). Door de sector te consulteren over de interpretatie van de bestaande normering en het toepassingsgebied ervan, kan worden bereikt dat voor alle partijen duidelijkheid ontstaat over de betekenis van de normen die betrekking hebben op nummeridentificatie.

2.4. De respons

Op de consultatie hebben voldoende partijen gereageerd om te kunnen spreken van een reactie van de sector. In Bijlage 1 zijn enige kwantitatieve gegevens over de respons opgenomen.

2.5. Normering, voorlichting en handhaving

De consultatie heeft geleid tot een verheldering van normen. De resultaten van de consultatie worden aan de sector bekend gemaakt en gepubliceerd op de website van het CBP. Het CBP zal zich bij het uitoefenen van zijn toezichthoudende taak mede baseren op de door de consultatie bereikte normering.

3. Inleiding bij de terugkoppeling

3.1. Inleiding

In de hoofdstukken 4 tot en met 16 volgt een uitwerking bij elk van de vragen uit het consultatiedocument. Deze omvat per onderwerp zowel een gemotiveerde bespreking van de reacties van de sector als resulterende CBP-zienswijzen.

3.2. Gehanteerde begrippen en afkortingen

In dit document komen de volgende afkortingen van wetten, regelingen en richtlijnen voor.

Met 95/46/EG wordt bedoeld de Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG 1995 L 281/31), ook genoemd de algemene privacyrichtlijn.

Onder Richtlijn 2002/58/EG wordt verstaan de Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 7 maart 2002 van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (PB L 201/37 (31.07.2002)), ofwel de bijzondere privacyrichtlijn.

De Wet implementatie Europees regelgevingskader voor de elektronische communicatiesector is op 19 mei 2004 in werking getreden (Staatsblad 2004, 189; zie ook het Inwerkingtredingsbesluit in Staatsblad 2004, 207). Door deze wet worden de richtlijnen in de Telecommunicatiewet van 1998 geïmplementeerd, zij het dat de implementatie van de richtlijnen ook gedeeltelijk (en gelijktijdig) plaatsvindt via algemene maatregelen van bestuur (AMvB's) en ministeriële regelingen.

Onder Tw wordt verstaan de Wet van 19 oktober 1998 houdende regels inzake de telecommunicatie (Telecommunicatiewet), versie geldig vanaf 19 mei 2004.

RUDE staat voor de Regeling universele dienstverlening en eindgebruikersbelangen van 10 mei 2004, Staatscourant 2004, nr. 92, p. 11.

BUDE is Besluit universele dienstverlening en eindgebruikersbelangen, Staatsblad 2004, 203.

WBP staat voor de Wet bescherming persoonsgegevens.

Indien hieronder zonder nadere toelichting wordt gesproken van ‘de dienst’, dan wordt daarmee bedoeld de dienst nummeridentificatie zoals geformuleerd in artikel 1.1, onder cc, sub 1 Tw.

3.3. Leeswijzer

Dit terugkoppelingsdocument kent het in november 2003 gepubliceerde consultatiedocument als uitgangspunt. Om te bereiken dat sectorreacties voldoende duidelijk naar voren komen, worden de in het consultatiedocument gehanteerde contextbeschrijvingen, vraagformuleringen en voorgestelde zienswijzen niet steeds uitgebreid herhaald. Aangezien de desbetreffende teksten veel ruimte vragen, zouden ze te zeer de aandacht op zich vestigen. Door deze keuze is het, om tot waardering van de analyses te kunnen komen, soms nodig om het consultatiedocument te raadplegen .
Het consultatiedocument, waarin achtergronden bij de vragen zijn vermeld, is beschikbaar op de website www.cbpweb.nl van het CBP.

De voor u liggende tekst concentreert zich op de bespreking van de vraagstellingen, de daarbij geuite zienswijzen en de daaruit resulterende normering. Daarbij wordt de volgorde aangehouden die ook in het consultatiedocument is gehanteerd, zij het dat sommige vragen

gegroepeerd worden behandeld. In hoofdstuk 11 wordt, wellicht ten overvloede, ingegaan op de samenhang tussen de WBP en de Tw, dit ter inleiding van de hoofdstukken die ingaan op de informatieplicht.
Na de inhoudelijke, onderwerpsgewijze bespreking wordt van de onderwerpen die betrekking hebben op de informatieplicht een samenvatting gegeven.
In Bijlage 1 worden enige kwantitatieve gegevens over de consultatie gepresenteerd en in Bijlage 2 wordt ingegaan op de overlappende bevoegdheden van OPTA en het CBP, waar het gaat om onderwerpen die aan de orde komen in hoofdstuk 11 van de Telecommunicatiewet.

3.4. Opmerkingen

Het CBP merkt het volgende op:

- De in de Tw genoemde blokkeringsmogelijkheden zijn een waarborg ter bescherming van de persoonlijke levenssfeer, behorende bij het aanbieden van de dienst nummeridentificatie. Voor verstrekkingen van nummers waarvoor artikel 11.9 Tw geen toepassing vindt, is de WBP van toepassing, behoudens de gevallen waarin het nummer niet een geïdentificeerde of identificeerbare natuurlijke persoon betreft. Van deze samenhang is in hoofdstuk 11, en wel in het kader van informatieplichten, een preciezere uitwerking gegeven.
- Met het van kracht worden van de RUDE is de Regeling nummeridentificatie uit 1998 ingetrokken (artikel 5.1 RUDE).
- Ten tijde van de consultatie zijn mogelijk niet alle respondenten op de hoogte geweest van de (concept)tekst van de RUDE, die in mei 2004 verscheen. De reacties van de sector moeten tegen deze achtergrond gewaardeerd worden.

4. Eenduidigheid van het nummerbegrip bij ISDN-aansluitingen

4.1. Inleiding

Het eerste gedeelte van de consultatie betrof de reikwijdte van het begrip nummeridentificatie. Het is volgens het CBP van belang dat uitgesproken wordt wanneer er van nummeridentificatie sprake is bij diensten zoals SMS en internettelefonie. Daarnaast doet zich, vooral in situaties waarbij er per aansluiting meerdere nummers in het spel zijn, zoals ISDN, de vraag voor op welke nummers de dienst nummeridentificatie ziet.

4.2. Nummeridentificatie en ISDN

(vraag 1)
Bij het toepassen van bepalingen uit de Tw moet invulling worden gegeven aan de in de wet gehanteerde begrippen. Bij ISDN betekent dit in het bijzonder dat duidelijk gemaakt moet worden wat de reikwijdte van het begrip nummeridentificatie is en welke uitleg er vervolgens moet worden gegeven aan bepalingen in artikel 11.9 Tw.

De sector heeft aangegeven dat aan ISDN-abonnees per netwerkaansluitpunt meerdere, minstens twee, nummers ter beschikking worden gesteld, waarvan er één als hoofdnummer wordt aangemerkt[1]. Voor het onderstaande is het relevant te weten dat er bij ISDN niet wordt gesproken van 'lijnen', maar van kanalen. Per ISDN-netwerkaansluitpunt bestaan er meerdere, minstens twee, communicatiekanalen (B-kanalen) en een signaleringskanaal (D-kanaal). De verstrekking van nummers in het kader van de dienst geschiedt onveranderlijk via het D-kanaal.

Gelet op artikel 1.1., onder cc, sub 1 Tw valt de verstrekking van het nummer van een oproepend aansluitpunt dan wel van een nummer waarmee een individuele gebruiker kan worden geïdentificeerd, onder het begrip nummeridentificatie voor zover deze verstrekking plaatsvindt voordat de verbinding tot stand wordt gebracht. Daarbij wordt geen onderscheid gemaakt naar de van toepassing zijnde technologie. Ook kent de wet geen kwalificatie 'hoofdnummer'.

Omdat een ISDN-aansluiting meerdere nummers heeft, is, ook volgens respondenten, niet eenduidig wat onder 'het' nummer van een ISDN-netwerkaansluitpunt moet worden verstaan. Waar het gaat over de toepassing van bepalingen uit 11.9 Tw, is het in de opvatting van het CBP bij ISDN echter niet nodig om hiervan een nadere definitie te geven. Immers, uit de in artikel 1.1., onder cc, sub 1 Tw genoemde zinsnede 'dan wel een nummer waarmee een individuele gebruiker kan worden geïdentificeerd' is duidelijk dat de reikwijdte van de definitie van nummeridentificatie bij ISDN niet slechts een enkel, tevoren gedefinieerd nummer betreft. De dienst nummeridentificatie is daarmee niet beperkt tot hetgeen wat door de sector is genoemd 'het hoofdnummer', dat als default geldt voor gebruik door de dienst. Ook sommige respondenten gaven aan dat elk ander MSN-nummer[2] dan het hoofdnummer kan worden aangemerkt als nummer waarmee de gebruiker kan worden geïdentificeerd.

[1] Hoe de bepaling van het hoofdnummer tot stand komt en in welke mate deze bepaling afhangt van het type van ISDN-aansluiting doet minder ter zake. Bij een ISDN2-aansluiting (lees ISDN Basic Rate Interface; beschikbaar zijn twee communicatiekanalen) kan bijvoorbeeld het eerste nummer als hoofdnummer gelden, bij ISDN30 (lees ISDN Primary Rate Interface; beschikbaar zijn -bij toepassing in Europa- doorgaans 30 communicatiekanalen) kan als hoofdnummer worden aangemerkt het nummer dat is opgegeven bij de abonnementsaanvraag, en vergelijkbaar voor types die aangemerkt kunnen worden als ISDN-meervoudig (lees: types waarvoor andere aantallen communicatiekanalen bestaan dan bij ISDN2 of ISDN30).
[2] MSN = Multi Subscriber Numbering. Een ISDN-aansluiting kent meerdere nummers, elk ervan heet een MSN-nummer.

Verstrekking van enig MSN-nummer aan het oproepende netwerkaansluitpunt voordat de verbinding tot stand wordt gebracht kan daarmee worden aangemerkt als nummeridentificatie in de zin van de wet. Artikel 11.9 Tw is daarop steeds van toepassing. In de consultatie zijn hierover geen andere opvattingen naar voren gebracht.

De vraag is nu welke mogelijkheden er bij ISDN precies moeten worden geboden om de verstrekking van nummers te verhinderen. Sommige respondenten geven aan dat kostenoverwegingen mede bepalend zijn voor aan te bieden blokkeringsmogelijkheden; ook worden hier technische mogelijkheden en de praktische uitvoerbaarheid genoemd. Anderen hebben aangegeven niet verder te willen gaan dan vereist is in de wet.

Het CBP komt tot de volgende analyse.
Een gebruiker heeft op grond van artikel 11.9, eerste lid onder a Tw het recht om de doorgifte te verhinderen van het enkele, bij de oproep horende, nummer (ongeacht of dat het hoofdnummer is of een ander MSN-nummer) dat in het kader van nummeridentificatie aan een opgeroepen netwerkaansluitpunt wordt verstrekt. Dit recht ziet op het voor iedere oproep afzonderlijk blokkeren van nummerverstrekkingen.

Waar het gaat om de aan abonnees aangeboden mogelijkheden, wordt in artikel 11.9, eerste lid, onder a Tw, gesproken van het per afzonderlijke abonneelijn kunnen blokkeren van de verstrekking van nummers van oproepende netwerkaansluitpunten dan wel nummers waarmee individuele gebruikers kunnen worden geïdentificeerd.

Het blokkeringsrecht van de abonnee heeft kennelijk betrekking op meerdere nummers tegelijk en wel per afzonderlijke abonneelijn. De betekenis van het element ‘voor elke afzonderlijke abonneelijn’ wordt niet volledig helder uit de wetsgeschiedenis. Blijkens de artikelsgewijze toelichting op de Wet implementatie Europees regelgevingskader voor de elektronische communicatiesector 2002 is artikel 11.9, eerste lid, onder a Tw in zoverre gewijzigd dat daarin ook de in artikel 8, eerste lid, van Richtlijn 2002/58/EG voorziene mogelijkheid is opgenomen voor de oproepende abonnee om per afzonderlijke (abonnee)lijn de weergave van het oproepende nummer te blokkeren (Kamerstukken II, 28 851, nr. 3, p. 161). Hieruit valt niet meer op te maken dan dat het gaat om een blokkering per lijn, die niet noodzakelijk ook de abonneelijn behoeft te zijn. Dat zou in het geval van ISDN impliceren dat het blokkeringsrecht van de abonnee niet noodzakelijkerwijs betrekking heeft op de abonneeaansluiting als geheel, maar op elke afzonderlijke lijn die daarvan deel uitmaakt.

In artikel 8, eerste lid Richtlijn 2002/58/EG wordt gesproken van “preventing the presentation of the calling line identification on a per-line basis”. In de Nederlandse tekst is sprake van de mogelijkheid om te verhinderen dat het oproepende nummer wordt weergegeven voor elke afzonderlijke lijn.
Overweging 34 van de Richtlijn biedt evenmin veel nadere aanknopingspunten. Daar is sprake van “privacy options which are offered on a per-line basis”.

Binnen het kader van de dienst moet, naar de mening van het CBP, de verplichting tot het aanbieden van een lijnblokkering zo worden uitgelegd dat aan de abonnees ten minste de mogelijkheid dient te worden geboden om alle nummers betreffende een (abonnee)lijn te blokkeren, zonder dat daarbij per oproep nog een handeling behoeft te worden verricht. Dit betekent dat een aanbieder van ISDN aan zijn abonnees ten minste de mogelijkheid dient aan te bieden tot het blokkeren van alle nummers van het netwerkaansluitpunt tegelijk.

Een verder gaande interpretatie zou zijn dat per ISDN-kanaal afzonderlijk een lijnblokkering zou moeten worden geboden. Gelet op de omstandigheid dat bij gebruik van de ISDN-aansluiting niet tevoren kan worden bepaald welk kanaal daadwerkelijk wordt gebruikt bij het doen van een

oproep, ligt die interpretatie niet voor de hand.[3] Bovendien zou een dergelijke zienswijze niet aansluiten bij het streven naar een techniekonafhankelijke regulering.

Of, in het in het geval van ISDN, het in de Tw geformuleerde recht van de abonnee om de verstrekking van het nummer voor elke abonneelijn te blokkeren ook het recht omvat om die verstrekking voor elk nummer afzonderlijk te verhinderen, zal uiteindelijk dienen toe worden bepaald door OPTA, dan wel de rechter.
Daarmee is het vooralsnog aan de aanbieders om dergelijke mogelijkheden aan te bieden of niet.

Als uit artikel 11.9, eerste lid, onder a Tw naar het oordeel van OPTA dan wel de rechter de verplichting mocht voortvloeien om abonnees wél de mogelijkheid te bieden om voor elk afzonderlijk nummer aan te geven of de verstrekking van dat nummer geblokkeerd moet worden, dan kan daarvan uiteraard niet worden afgezien om redenen van kosten of operationele omstandigheden.

4.3. Keuze door abonnee

De Tw schrijft niet voor dat abonnees mogen bepalen welke van de bij het ISDN-aansluitpunt behorende nummers verstrekt mogen worden. Wel gelden er, gelet op artikel 11.9 Tw, aanspraken op het kunnen blokkeren van nummerverstrekkingen; niet alleen voor de abonnee, maar ook voor de gebruiker. Waar het gaat over mogelijkheden om aan te geven welke nummers in het kader van de dienst verstrekt mogen worden, kan het volgens de sector inderdaad zinvol zijn om de abonnee een keuzevrijheid te geven. Hierboven is aangegeven dat een van de nummers die horen bij een ISDN-aansluiting kan worden aangewezen als hoofdnummer. Zolang de abonnee geen specifieke andere keuze maakt, zal de dienst nummeridentificatie werken met het hoofdnummer.

Vanuit (kosten)technisch oogpunt is het door abonnees zelf kunnen instellen van dit nummer een realistische optie, die bij sommige aanbieders reeds voorhanden is. Een enkele aanbieder is van mening dat de markt niet dient te worden verplicht om extra toepassingen aan te bieden waartoe zij op basis van de Tw niet verplicht is. Het CBP sluit zich bij deze laatste zienswijze aan.

[3] Terwijl er bij een ISDN-aansluiting meerdere nummers horen, is het niet zo dat er een vaste relatie is tussen het nummer waarmee een oproep tot stand komt en enig kanaal waarover de bijbehorende communicatie wordt afgewikkeld. Het is daarom niet zinvol om nummerverstrekkingen te willen reglementeren via het aanbieden van blokkeringsmogelijkheden per (B-)kanaal.

5. Nummeridentificatie bij SMS

5.1. Inleiding

(vragen 2 en 3)
Het bijzondere regime van artikel 11.9 Tw kan volgens het CBP niet zonder meer van toepassing worden geacht bij andere diensten dan vaste en mobiele telefonie. Een van de diensten die hier nadere beschouwing verdient is SMS.

De sector is vrijwel zonder uitzondering van mening dat het meezenden van het oproepende nummer bij SMS niet valt onder de reikwijdte van het begrip 'nummeridentificatie', zoals gedefinieerd in artikel 1.1 Tw. Volgens de definitie in artikel 1.1, onder cc, sub 1 Tw moet er sprake zijn van verstrekking van een nummer aan het opgeroepen netwerkaansluitpunt voordat de verbinding tot stand wordt gebracht. Het begrip 'oproep' is gedefinieerd in artikel 11.1, onder f Tw en betreft een door middel van een openbare telefoondienst tot stand gebrachte verbinding die zonder noemenswaardige vertraging communicatie tussen gebruikers of abonnees over en weer mogelijk maakt.

Een respondent meende, zonder dit nader te motiveren, dat het verzenden het nummer bij SMS-berichten wel onder de reikwijdte van artikel 11.9 Tw valt. Ook een enkele aanbieder van mobiele telefonie is die mening toegedaan, aangevend dat er bij een verzending die plaats vindt via een GSM-verbinding, sprake is van een openbare telefoondienst en het een nummer betreft waarmee de individuele gebruiker kan worden geïdentificeerd.

Het overgrote deel van de respondenten stelt zich op het standpunt dat een SMS-bericht geen oproep is in de zin van artikel 11.1 Tw. De argumenten lopen evenwel uiteen. Bij SMS zou geen sprake zijn van een oproep, omdat niet voldaan wordt aan de daarvoor in artikel 11.1, onder f Tw genoemde eisen 'zonder noemenswaardige vertraging' en 'over en weer'. Andere respondenten wezen er op dat er bij SMS, dat gebruik maakt van het signaleringskanaal, geen sprake is van het tot stand komen van een verbinding, of althans niet van een verbinding waarover communicatie over en weer mogelijk is.
Andere aanknopingspunten werden gevonden in de definitie van het begrip 'gesprek', dat bepalend is voor het begrip openbare telefoondienst, zoals gedefinieerd in artikel 1, onder x Tw. Meerdere respondenten meenden dat de wetgever met 'gesprek' gedoeld heeft op spraakverkeer en dus niet op SMS, dat in één reactie aangemerkt werd als een 'datadienst', met de aantekening dat SMS berichten onder omstandigheden wel kunnen worden omgezet naar spraak. Eén respondent vergeleek het verzenden van een SMS-bericht met het versturen van een MMS-bericht en met het versturen van een e-mail, waardoor er ook geen sprake zou zijn van een oproep.

5.2. Toepassing WBP

Naar de opvatting van het CBP is er alleen al omdat bij SMS-diensten geen nummers worden verstrekt voordat de verbinding tot stand wordt gebracht, geen sprake van het aanbieden van nummeridentificatie als bedoeld in artikel 1.1, onder cc, sub 1 Tw. Artikel 11.9 Tw is derhalve niet van toepassing. Bovendien is het de vraag in welke mate er bij de *store-and-forward* toepassing[4] SMS überhaupt sprake is van een verbinding. De overige argumenten behoeven daarmee hier geen verdere bespreking. Het ligt eerder op de weg van OPTA om invulling te geven aan begrippen als oproep, openbare telefoondienst en dergelijke. Voor het CBP is slechts van belang vast te stellen welk regime van toepassing is op de verstrekking van nummers in het geval van SMS-berichten. Dat is, naar het CBP meent, niet dat van de Telecommunicatiewet, maar mogelijk wel dat van de WBP.

[4] SMS-aflevering gaat via een mechanisme waarbij het bericht naar een Short Message Service Centre (SMSC), gezonden wordt dat het doorzendt naar het bestemmingsapparaat.

Indien het oproepende nummer, dat bij SMS aan de geadresseerde wordt verstrekt, een persoonsgegeven is, zal op het meezenden van dat nummer de WBP van toepassing zijn. Een persoonsgegeven is volgens de definitie in artikel 1, onder a WBP elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Een verstrekking door middel van doorzending is blijkens de definitie in artikel 1, onder b WBP aan te merken als een verwerking van persoonsgegevens.
In 1994 heeft de voorganger van het CBP, de Registratiekamer, geoordeeld dat het verstrekken van het telefoonnummer in het kader van nummeridentificatie is aan te merken als het verstrekken van een persoonsgegeven (uitspraak 93.A.012 van 25 februari 1994). In lijn met die uitspraak meent het CBP dat verstrekking van het nummer van de verzender van een SMS-bericht aan de ontvanger is gebaseerd op de vooronderstelling dat deze aan de hand van dat nummer kan weten met wie hij van doen heeft. Deze wetenschap kan berusten op een eigen registratie van de ontvanger, zoals een telefoonlijstje in diens toestel. Daarnaast zullen de verzenders van SMS-berichten zich dikwijls in het bericht zelf als afzender bekend maken. Ook zal door het bericht te beantwoorden in veel gevallen de identiteit van de afzender zijn vast te stellen. Dit leidt tot het inzicht dat het meezenden van het oproepende nummer aan de geadresseerde bij SMS-berichten veelal is aan te merken als de verstrekking van een persoonsgegeven, waarop dientengevolge de WBP van toepassing is.

5.3. Een WBP-grondslag

Voor verstrekkingen van persoonsgegevens dient een grondslag te bestaan als bedoeld in artikel 8 WBP.
Een respondent heeft zich waar het gaat om het weergeven van het nummer op het standpunt gesteld dat hiervoor niet de algemene regel uit hoofde van de WBP zou moeten gelden dat daarvoor de expliciete goedkeuring van de klant nodig is.
Naar het CBP meent is de ondubbelzinnige toestemming van de abonnee als bedoeld in artikel 8, onder a WBP waaraan de betreffende respondent kennelijk refereert, niet de enige grond die de gegevensverstrekking kan rechtvaardigen. De grondslag voor verstrekking zou in beginsel ook kunnen worden gevonden in de bepalingen van artikel 8, onder b dan wel van artikel 8, onder f WBP.

Wat de b-grond betreft dient te worden nagegaan of de gegevensverwerking noodzakelijk is voor de uitvoering van de overeenkomst waarbij de betrokkene partij is. Van belang bij die beoordeling zijn de eventuele mogelijkheden om geblokkeerde nummers bij SMS-verkeer niet door te geven aan het ontvangende randapparaat. De respons vanuit de sector op de desbetreffende vraag (vraag 3) is niet eenduidig. Meerdere respondenten hebben aangegeven technische mogelijkheden te zien om een SMS-bericht af te leveren zonder nummerpresentatie, maar achten het niet aan de orde dan wel onwenselijk om nummerweergave bij SMS te blokkeren. Een aanbieder van mobiele telefonie zonder eigen netwerk zegt zich wel voor te kunnen stellen dat netwerkaanbieders in staat zijn om in het SMS-protocol aan te geven of de verzender een (voor weergave) geblokkeerd nummer heeft. Een ander stelt dat het blokkeren op dit moment niet wordt ondersteund door het netwerk.
Anderen zien daarentegen geen technische mogelijkheden of geven aan dat ten gevolge van de techniek die bij SMS wordt gebruikt het nummer van de verzender altijd wordt weergegeven aan het ontvangende randapparaat.
Het CBP meent uit de respons te kunnen afleiden dat verstrekking van het oproepende nummer aan het ontvangende randapparaat niet noodzakelijk is voor het verzorgen van een SMS-oproep. Dat zou betekenen dat voor de verstrekking van dat nummer bij SMS-verkeer geen grondslag kan worden gevonden in artikel 8, onder b WBP.
Een respondent was van mening dat SMS zou moeten worden vergeleken met diensten zoals MMS en e-mail. De convergentie van deze diensten zou maken dat regels over het blokkeren van nummerdoorgifte bij SMS niet aan de orde zijn, omdat deze bij e-mail en ook MMS geen toepassing vinden.

Volgens het CBP gaat voor MMS-berichten hetzelfde op als voor SMS. E-mailverkeer kan daarentegen niet bij de ontvanger worden afgeleverd zonder IP-adres van de verzender. In het geval van e-mail kan voor de verstrekking wel een grondslag worden gevonden in artikel 8, onder b WBP; in geval van MMS daarentegen niet.

Artikel 8, onder f WBP kan de verstrekking rechtvaardigen indien die gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert. Volgens de wetsgeschiedenis van de WBP moet in dit kader worden afgewogen of er een noodzaak bestaat tot verstrekking met het oog op een gerechtvaardigd belang van de verantwoordelijke of van de verkrijgende derde. Daarnaast dienen de belangen van de betrokkene afzonderlijk te worden gewogen. De belangen van betrokkene zullen minder gewicht in de schaal leggen naarmate in zijn belang meer waarborgen voor een zorgvuldig gebruik van zijn gegevens zijn gesteld (Kamerstukken II, 25 892 nr. 3, p. 88). Verschillende respondenten achtten het onwenselijk dat de verzender van het SMS-bericht zich tegen nummerweergave zou kunnen verzetten. De daarvoor aangevoerde argumenten komen er op neer dat het in het belang van de geadresseerde van een SMS-bericht zou zijn om geen anonieme SMS-berichten te ontvangen, waaronder SMS-spam en plaagberichten. Het CBP acht dit op zichzelf gerechtvaardigde belangen, maar ziet daarin nog geen rechtvaardiging om steeds het nummer van de verzender van een SMS-bericht te verstrekken aan de ontvanger. Immers, op grond van artikel 11.7, derde lid Tw dient een SMS-bericht voor commerciële, ideële of charitatieve doeleinden de werkelijke identiteit van de afzender te vermelden en ook een adres waar de ontvanger een verzoek tot beëindiging kan indienen. Volgens artikel 11.11 Tw kunnen abonnees die last ondervinden van hinderlijke SMS-berichten, hun aanbieder verzoeken de naam en adresgegevens van de oproepende abonnee te verstrekken. Daarmee kan nummerweergave niet meer noodzakelijk worden geacht voor de genoemde belangen van de ontvanger. Anderen wezen op belangen van de aanbieder zelf. Er zouden beperkingen zijn aan de toepasbaarheid van artikel 11.9 Tw op communicatiemiddelen die wellicht functioneel gezien gelijksoortig zijn aan geschakelde telefoonverbindingen, maar gebruik maken van andere technieken. Volgens de sector spelen hier bedrijfseconomische en financiële redenen een rol. Blijkens de wetsgeschiedenis kunnen verantwoordelijken verwerkingen die voor een behoorlijke functioneren van een commercieel bedrijf noodzakelijk zijn, baseren op de grondslag genoemd onder artikel 8, onder f WBP, zolang is rekening gehouden met de gerechtvaardigde belangen van betrokkenen (Kamerstukken II, 25 892, nr 6, p. 17).

Naar de opvatting van het CBP dient de aanbieder, gelet op het vorenstaande, ook bij SMS-berichten de verstrekking van het nummer van de oproeper te voorzien van waarborgen. Naar analogie met artikel 11.9 Tw kan daarbij worden gedacht aan waarborgen in de sfeer van blokkeringen en het informeren van de betrokkene. Indien het in technisch opzicht bij SMS niet mogelijk is de verstrekking van het oproepende nummer te blokkeren, zal de aanbieder andere waarborgen dienen te stellen, om een grondslag voor de verstrekking te kunnen vinden in artikel 8, onder f WBP. Anders zal alleen een grondslag voor de verstrekking kunnen worden gevonden in artikel 8, onder a WBP. In dat geval zou de oproepende SMS-gebruiker voor de verstrekking zijn ondubbelzinnige toestemming dienen te geven na daarover door de aanbieder te zijn geïnformeerd. Het CBP adviseert de aanbieders zich nader hierop te beraden.

6. Nummeridentificatie bij internetdiensten

6.1. Inleiding

(vraag 4)
In de consultatie heeft het CBP aandacht geschonken aan de vraag in welke gevallen er bij internettelefonie sprake is van de dienst nummeridentificatie in de zin van artikel 1, onder cc Tw. Omdat niet het gebruikte netwerk bepalend is voor het van toepassing zijn van regelgeving, hangen oordelen hierover niet vooral af van de mate waarin communicatie geheel of gedeeltelijk tot stand komt via signaaloverdracht over het internet.
Het CBP streeft er thans niet naar om vast te stellen in welke mate verschijningsvormen van internettelefonie onder de reikwijdte van de Tw vallen. Een volledige inventarisatie en analyse van die verschijningsvormen is niet opportuun; hier zijn slechts de bepalingen uit de Tw rond nummeridentificatie aan de orde.

6.2. Internettelefonie

De sector is gevraagd in welke mate artikel 11.9 Tw ziet op VoIP[5], zonder dat daarbij expliciet door het CBP was aangegeven welke verschijningsvorm van internettelefonie daarmee werd bedoeld.

Het CBP merkt op dat sommige respondenten bij de beantwoording van de vragen over VoIP vooral een uitspraak hebben willen doen over de toepasselijkheid van artikel 11.9 Tw op internetspraakdiensten, terwijl andere zich geconcentreerd hebben op de vraag of artikel 11.9 Tw ook van toepassing zou kunnen zijn op andere internetdiensten dan VoIP.

Enige respondenten meenden dat de internetdienst VoIP onder artikel 11.9 Tw zou kunnen vallen. Daarbij werd opgemerkt dat deze zienswijze ook geldt voor VoDSL[6], temeer daar er ook bij VoDSL geen onderscheid meer bestaat tussen spraakgedeelten en datagedeelten.
Van degenen die meenden dat VoIP onder de reikwijdte van artikel 11.9 Tw valt, stelden enigen dat uit de nieuwe Tw kan worden afgeleid dat elke vorm van communicatie, dus ook VoIP, onder artikel 11.9 Tw kan worden geschaard, omdat dit artikel zou zien op openbare elektronische communicatienetwerken dan wel -diensten, en dus niet alleen op spraak. Hierbij werd opgemerkt dat bijvoorbeeld ook een IP-adres binnen de definitie van nummeridentificatie kan vallen.
Andere voorstanders beargumenteerden hun zienswijze via de elementen ‘spraak’ en ‘openbare telefoondienst’.
De respondent die twijfelde stelde dat er bij ‘het aanbieden en bij de werking van internetdiensten’ niet steeds sprake is van een oproep waarbij de verstrekking van het nummer plaatsvindt voordat er verbinding tot stand wordt gebracht. Op het moment dat IP-adressen worden verstrekt gebeurt dit met het doel om de communicatie zelf mogelijk te maken, niet voorafgaand aan de communicatie. In deze reactie werd aangegeven dat nader onderzoek nodig is om te bepalen of bij VoIP artikel 11.9 Tw van toepassing is.

Er is ook een respondent die vindt dat artikel 11.9 Tw niet van toepassing kan zijn op VoIP. VoIP is volgens hem louter een applicatie die via het internet kan worden gebruikt, te vergelijken met applicaties zoals *gaming* via het internet. In die optiek heeft een aanbieder (van een netwerk of telefoondienst) geen bemoeienis met het gebruik ervan. In deze zienswijze bieden de aanbieders enkel de fysieke verbinding alsmede de toegang tot het internet aan. Ook is gesteld dat waar er geen sprake is van een telefoondienst er ook geen sprake kan zijn van de dienst nummeridentificatie.

[5] VoIP (Voice over IP) wordt hier als een generieke aanduiding voor internettelefonie gebruikt.
[6] Voice over DSL. DSL (Digital Subscriber Line) maakt snel transport van data en spraak mogelijk, inclusief internetconnectivity, over bestaande telefoonlijnen.

Overigens werd opgemerkt dat de plicht om te voldoen aan de bepalingen van artikel 11.9 Tw beperkt wordt door de technische haalbaarheid en de financieel-economische gevolgen ervan en ook dat de reikwijdte van de WBP beperkt is tot nummergegevens die herleidbaar zijn tot een natuurlijk persoon.

Deze reacties overziend komt het CBP tot de volgende zienswijze.
Er bestaan verschillende architecturen voor het transporteren van spraak middels internettelefonie. Daarbij is het overbrengen van spraak door initiatieven van individuele gebruikers zónder dat daarbij een specifieke internettelefonie-dienstverlener is betrokken, slechts een van de varianten. In varianten waarin een dergelijke internettelefonie-dienstverlener wél een rol speelt kan men een classificatie aanbrengen naar de mate waarin het mogelijk is om abonnees met een PSTN-netwerkaansluitpunt[7] te bereiken. Welke regelgeving voor de bescherming van de persoonlijke levenssfeer van toepassing is op een verschijningsvormen van internettelefonie, wordt mede bepaald door de mate waarin oproepen naar abonnees van reguliere telefoondiensten mogelijk zijn.

De grote variatie aan verschijningsvormen van internettelefonie maakt dat er door het CBP geen categorische uitspraak kan worden gedaan over het van toepassing zijn van Tw-bepalingen op dergelijke diensten. Ook de reacties van de sector deden dit vermoeden.

Hier gaat het om de vraag in hoeverre artikel 11.9 Tw op dergelijke diensten van toepassing is. Uitspraken daarover verlangen dat er ingegaan wordt op de elementen
- openbaarheid;
- het verstrekken van nummers;
- telefoondienst;
- voordat de verbinding tot stand komt;
- oproep.

De **openbaarheid** van een dienst hangt af van de beschikbaarheid ervan voor het publiek, te onderscheiden van de beschikbaarheid ervan voor besloten groepen. De beschikbaarheid kan worden bepaald aan de hand van criteria, waaronder
- de mate van standaardisatie van het proces, zodat dat door verschillende aanbieders kan worden verzorgd;
- de gerichtheid van het aanbod op een breed publiek tegen vergelijkbare voorwaarden.

In de regel zal bij VoIP aan dergelijke criteria zijn voldaan en is voldaan aan het element van openbaarheid.

Verder moet vastgesteld worden of er bij internettelefonie sprake is van het **verstrekken van nummers**. Omdat bepalingen rond nummeridentificatie uit de Tw zich niet beperken tot verstrekkingen van telefoonnummers, kan onder omstandigheden ook het verstrekken van een IP-adres maken dat de bepalingen rond nummeridentificatie van toepassing zijn. Onder het begrip ‘nummer’ wordt volgens artikel 1, onder bb Tw immers verstaan: “cijfers, letters of andere symbolen, al dan niet in combinatie, die bestemd zijn voor toegang tot of identificatie van gebruikers, netwerkexploitanten, diensten, netwerkaansluitpunten of andere netwerkelementen”. Deze verstrekking van nummers moet dan nog, wegens de definitie van ‘oproep’ in artikel 11.1, onder f Tw, gerelateerd zijn aan een **telefoondienst**.
Een mogelijke uitzondering, vergelijkbaar met andere ongedifferentieerde internettoepassingen die niet onder het bijzondere regime zullen vallen, bestaat voor de VoIP-variant waarbij van spraak over een datanetwerk door initiatieven van individuele gebruikers wordt overgebracht zonder dat daarbij een specifieke VoIP-dienstverlener is betrokken. Deze variant is niet op te vatten als een ‘dienst’ waarbij VoIP wordt aangeboden. Eindgebruikers bepalen hier zelf hun communicatiemogelijkheden. Er is zonder bijzondere maatregelen geen communicatie mogelijk

[7] public switched telephone network, de concatenatie van de openbare (circuit-switched) telefonienetwerken.

met abonnees van de traditionele telefoondienst. Wel natuurlijk is hierbij een dienst nodig voor het transport van data over een netwerk.

Verder is bij VoIP-varianten waarbij spraak over een datanetwerk wordt overgebracht van belang om na te gaan of het verstrekken van nummers plaatsvindt **voordat de verbinding tot stand komt**. Dit is een bepalend element in de definitie van nummeridentificatie in artikel 1, onder cc, sub 1o Tw.

Ook is te bezien in welke mate er bij een VoIP-variant sprake is van een **oproep** in de zin van artikel 11.1 onder f Tw. Zonder dit is er geen sprake van oproepende en opgeroepen netwerkaansluitpunten. Het begrip 'oproep' op zijn beurt steunt op de definitie van 'openbare telefoondienst', dat wil zeggen een dienst die voor het publiek beschikbaar is voor uitgaande en binnenkomende gesprekken (artikel 1 onder x Tw);

VoIP-varianten anders dan de variant die door initiatieven van eindgebruikers wordt opgezet zullen naar het zich laat aanzien onder de reikwijdte van artikel 11.9 Tw vallen. Een nadere toets tegen onder meer de genoemde criteria zal, in overleg met OPTA, plaatsvinden indien een concrete variant van VoIP voorligt ter beoordeling.

6.3. Internetdiensten niet betreffende spraak

Het CBP heeft de sector ook willen consulteren over internetdiensten niet betreffende spraak, waarbij tegelijk met het bericht een nummer van de afzender wordt verstrekt aan de geadresseerde. Daarbij werd gevraagd naar zienswijze op de visie dat in die gevallen de WBP van toepassing is, en niet artikel 11.9 Tw.
Het CBP meende een zienswijze te kunnen baseren op enerzijds 'niet betreffende spraak' en anderzijds op het onderscheid tussen de woorden 'tegelijk', en 'voordat'. Dit onderscheid is blijkens de definitie van artikel 1.1, onder cc, sub 1 Tw relevant voor de vraag of er sprake is van nummeridentificatie.

De sectorreacties sloten helaas niet aan bij de intentie van de CBP-vraag.
Een respondent onderschrijft de visie van het CBP zonder meer, een ander stemt met het resultaat in op grond van het argument dat er in de gegeven situatie in het geheel geen sprake is van een oproep.
Een aantal respondenten is van mening dat in het genoemde geval de WBP naast de Tw van toepassing zal kunnen zijn, zonder daarbij in te gaan op de relevantie van de begrippen 'spraak' en 'voordat'. Hierbij werd niet uitgesloten dat concrete toepassingen van geval tot geval moeten worden bezien. De door het CBP gebruikte bewoordingen waren voor drie respondenten aanleiding om te benadrukken dat de WBP relevant is voor nummers die aan te merken zijn als persoonsgegeven, dat wil zeggen herleidbaar zijn tot een natuurlijk persoon.
Ten slotte zijn er respondenten die vinden dat alleen de Tw van toepassing kan zijn en niet de WBP, waaraan men niet toe zou komen nu internetdiensten binnen de reikwijdte van de Tw vallen. In paragraaf 3.4 is aangegeven hoe deze zienswijze beoordeeld moet worden.

Bij het geven van een reactie heeft de sector zich denkelijk geconcentreerd op andere aspecten dan het CBP. In gevallen waarin er geen sprake is van de dienst nummeridentificatie zal ook artikel 11.9 Tw niet van toepassing zijn. Voor zover er wel sprake is van het verstrekken van persoonsgegevens, daaronder mede te verstaan een tot een identificeerbare natuurlijke persoon te herleiden nummer, is volgens het CBP de WBP van toepassing.
Welnu, gelet op artikel 1, onder cc Tw is het 'verstrekken, voordat de verbinding tot stand wordt gebracht' een bepalend element om te kunnen spreken van nummeridentificatie.
In gevallen waarin, zoals in de vraagstelling, het nummer tegelijk met het bericht wordt verstrekt wordt er niet voldaan aan de eisen genoemd in het artikel. Dat betekent dus dat op de betreffende internetdiensten (waaronder bijvoorbeeld e-maildiensten) artikel 11.9 Tw niet van toepassing is maar de WBP.

7. Toedeling verantwoordelijkheden

7.1. Inleiding

(vragen 5 en 6)
Artikel 11.9 Tw richt zich tot de aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst die door middel van dat netwerk of als onderdeel van die dienst nummeridentificatie aanbiedt. Op de aanbieder van nummeridentificatie rusten de verplichtingen tot onder meer het voorlichten van gebruikers en abonnees alsmede tot het bieden van mogelijkheden tot blokkering van het verstrekken van nummers en weigering van oproepen waarvoor de nummerverstrekking is geblokkeerd.

7.2. Verantwoordelijkheden algemeen

Het CBP heeft de sector vragen voorgelegd over de verantwoordelijkheid voor het verstrekken van het nummer. Twee situaties zijn daarbij onderscheiden. Vraag 5 had betrekking op de situatie waarin de aanbieder van een vaste of mobiele telefoondienst niet beschikt over een eigen netwerk. Vraag 6 had betrekking op carrier select (CS) of carrier preselect (CPS) aanbieders. In beide situaties moet worden bepaald wie als aanbieder van de dienst nummeridentificatie dient te worden aangemerkt. Beide vragen worden hier in samenhang behandeld.

Het CBP is van mening dat ook wanneer de aanbieder van de telefoondienst niet beschikt over een eigen netwerk, deze verantwoordelijk is in de zin van de WBP voor de werking van nummeridentificatie en het in dat kader verstrekken van nummers aan opgeroepen aansluitpunten. De netwerkaanbieder die ten behoeve van de verantwoordelijke gegevens verstrekt in het kader van nummeridentificatie, moet worden aangemerkt als bewerker in de zin van de WBP.

Gevraagd naar de zienswijze van de sector over de verantwoordelijkheidsverdeling geeft het merendeel van de respondenten aan dat de aanbieder van de dienst nummeridentificatie de WBP-verantwoordelijke ervoor is. Waar het gaat over de positie van de netwerkaanbieder, geven meerdere respondenten aan dat deze slechts 'uitvoerder' is.

Volgens een enkeling geldt de netwerkaanbieder als verantwoordelijke, behalve waar het gaat om het informeren van klanten. Ook werd de mogelijkheid van een gezamenlijke verantwoordelijkheid naar voren gebracht, al werd in dit laatste geval aangetekend dat de verantwoordelijkheden op het gebied van informatieverstrekking wel bij de dienstenaanbieder zouden moeten liggen.
Een respondent formuleert het zo dat verplichtingen rond nummeridentificatie behoren bij de aansluiting (het abonnement): ‘De aanbieder die de aansluiting levert is […] verantwoordelijk.’

Eén respondent gaat specifiek in op de verantwoordelijkheidsverdeling bij het blokkeren van nummerdoorgiftes. Gesteld wordt dat hiervoor afspraken nodig zijn tussen de dienstenaanbieder en de netwerkaanbieder. Deze respondent geeft voorts aan dat er op netwerkniveau mogelijk geen sprake is van de verwerking van persoonsgegevens.

Het CBP handhaaft de zienswijze dat de dienstenaanbieder die door de eindgebruiker is gecontracteerd verantwoordelijk is voor de kwaliteit van de door hem geleverde diensten.
In termen van de WBP is dienstenaanbieder degene die het doel en de middelen van de verstrekking vaststelt. Daarmee is de dienstenaanbieder tevens de verantwoordelijke voor de gegevensverstrekking in de zin van de WBP. De netwerkaanbieder moet worden aangemerkt als bewerker, in de zin van artikel 1, onder e WBP, die ten behoeve van de verantwoordelijke gegevens verstrekt.

Artikel 3.3 van de RUDE legt aan aanbieders van openbare telefoonnetwerken en of openbare telefoondiensten de verplichting op om eindgebruikers de mogelijkheid van nummeridentificatie te bieden. Een verplichting tot het aanbieden leidt via artikel 11.9 Tw ook tot de verplichting om de in dat artikel genoemde blokkeringsmogelijkheden aan te bieden. In het geval van C(P)S: voor zover deze betekenis hebben.

Merk op dat de wetgever in artikel 3.3. van de RUDE wel de rollen onderscheidt, maar in het midden laat hoe de onderlinge verhouding tussen de aanbieder van de dienst en de aanbieder van het netwerk is. Het lijkt echter, ingaand op de suggestie dat er sprake is van een gezamenlijke verantwoordelijkheid, niet realistisch om een gedeelde verantwoordelijkheid tussen de netwerkaanbieder en de dienstenaanbieder te veronderstellen.

De aanbieder van de elektronische communicatiedienst (veelal de telefoondienst) zal ervoor moeten zorgen dat nummeridentificatie en de daarbij aan te bieden blokkerings- en weigeringsmogelijkheden door het netwerk waarover hij zijn diensten aanbiedt worden gerealiseerd. Dit zal hij contractueel of anderszins moeten overeenkomen met de netwerkaanbieder. De verplichtingen jegens de klant tot het aanbieden van blokkeringen alsmede het informeren berusten bij de aanbieder van de telefoondienst en niet bij de aanbieder van het netwerk.

De verantwoordelijkheid van de dienstenaanbieder impliceert niet dat deze geen afspraken zou kunnen maken met de netwerkaanbieder over de uitvoering van bepaalde verplichtingen. De dienstenaanbieder dient zijn klanten als dan te informeren over de mate waarin het voor een abonnee praktisch kan zijn zich te wenden tot de netwerkaanbieder, mocht zo een doorverwijzing in de rede liggen. Ongeacht eventueel gemaakte afspraken kan de aanbieder te allen tijde als verantwoordelijke door de eindgebruiker worden aangesproken. De netwerkaanbieder heeft mogelijk wel verplichtingen, jegens de dienstenaanbieder wel te verstaan!
In de praktijk blijkt dat de aanbieder van de dienst vragenstellers doorverwijst naar de aanbieder van het netwerk, terwijl daarna de aanbieder van het netwerk weer terugverwijst naar de aanbieder van de dienst. Gelet op het voorgaande dient de eindgebruiker telkens de dienstenaanbieder te kunnen aanspreken.

7.3. Verantwoordelijkheden bij carrierdiensten

Bij het aanbieden van carrierdiensten heeft de klant zowel een overeenkomst met een telefonieaanbieder als een overeenkomst met de C(P)S-aanbieder. Als bij het toewijzen van verantwoordelijkheden al volstaan zou kunnen worden met de vuistregel dat plichten toevallen aan degene met wie gecontracteerd is, dan zal toch op zijn minst moeten worden aangegeven welke plichten er voor welke contractant gelden.

De C(P)S-aanbieder en de aanbieder van de openbare telefoondienst verwerken beide het nummer waarmee de individuele gebruiker kan worden geïdentificeerd en zijn dan ook beide verantwoordelijk voor het informeren van de abonnees.
Voor de beantwoording van de vraag wie verantwoordelijk kan worden gehouden voor het aanbieden van nummeridentificatie kunnen er, met name in het geval van diensten waar C(P)S-aanbieders bij betrokken zijn, aanknopingspunten worden gevonden in de RUDE.
De wetgever heeft, gelet op het in artikel 3 van de RUDE gemaakte onderscheid naar aanbieders van carrierdiensten en aanbieders van openbare telefoondiensten, in elk geval voor wat betreft het informeren het belang van het expliciet maken van verplichtingen van betrokken partijen onderkend.

In het geval van C(P)S kunnen aanbieders van nummeridentificatie op grond van artikel 3.3., vierde lid, RUDE rekenen op de medewerking van de aanbieder van openbare elektronische communicatienetwerken die worden gebruikt om de carrierdienst aan te bieden.

Voor deze ‘verplichte CPS-gevallen’ zijn in de RUDE tevens de informatieverplichtingen uitgewerkt.

Uit de respons kwam niet duidelijk naar voren of zienswijzen betrekking hadden op verplichtingen tot het aanbieden van blokkeringsmogelijkheden dan wel op informatieverplichtingen. Verder is er ook niet gewezen op de onnauwkeurigheid in de CBP-vraagstelling. De vraag zoals in het consultatiedocument gesteld laat ruimte voor verschillende interpretaties. Men kan namelijk met ‘een gedeelde verantwoordelijkheid’ willen uitdrukken
a) dat er voor elke oproep / gesprek sprake is van een gedeelde verantwoordelijkheid;
b) dat verantwoordelijkheden, gezien over de totale collectie van oproepen / gesprekken, dan weer aan de ene dienstverlener, dan weer aan de andere toevallen, zonder daarbij een uitspraak te doen over een verantwoordelijkheidsverdeling per oproep / gesprek.

Het CBP bedoelde te vragen naar de interpretatie genoemd onder a).

De respondent die meende dat de C(P)S-aanbieder geen verantwoordelijke kon zijn motiveerde dit ondermeer door te wijzen op de technische uitvoering van de blokkering van nummerverstrekkingen die alleen door de netwerkaanbieder gerealiseerd kan worden. Het CBP wijst er op dat een dergelijke zienswijze strijdig is met artikel 3.3. van de RUDE, omdat daar een andere rolverdeling is aangegeven.

Er zijn ook aanbieders die denken aan een gezamenlijke verantwoordelijkheid van de C(P)S en netwerkaanbieder. Niet steeds was daarbij echter duidelijk welke interpretatie van de vraagstelling hier was gekozen.

De partij die meende dat juist uitsluitend de C(PS)-aanbieder verantwoordelijke kan zijn motiveerde dat de netwerkbeheerder te beschouwen is als een 'uitvoerder' van de faciliteit nummeridentificatie in opdracht van de dienstaanbieder.

Het CBP overweegt als volgt. Wanneer een abonnee gebruik maakt van C(P)S is er sprake van meerdere aanbieders van wie hij een dienst afneemt. Afhankelijk van de keuze van de abonnee wordt een gesprek de ene keer afgehandeld door de aanbieder van de openbare telefoondienst en de andere keer door de aanbieder van C(P)S.
Voorstanders van een gedeelde verantwoordelijkheid die in hun reactie lieten blijken de eerste interpretatie van de vraag voor ogen te hebben gehad, stelden dat in beide situaties de “afhandelende” aanbieder is aan te merken als verantwoordelijke voor de gegevensverwerking in de zin van de WBP. Hierbij werd opgemerkt dat er in laatstgenoemde situatie (afhandeling door C(P)S) tevens sprake is van een bewerker (in de gedaante van de faciliterende netwerkaanbieder).
Per gesprek geldt er, vanuit de optiek van de abonnee, precies één partij als verantwoordelijke.
Het CBP sluit zich bij deze zienswijze aan en komt daar mee terug van de CODO-zienswijze. Merk op dat er, in lijn met de bepalingen in de RUDE, geen sprake is van een gezamenlijke verantwoordelijkheid.

8. Aanvragen permanente blokkering bij carrierdiensten

8.1. Inleiding

(vraag 7)
In artikel 11.9, onder a, Tw wordt gesproken over het per abonneelijn blokkeren van verstrekkingen van nummers. Vraag 7 uit de consultatie had als onderwerp wie bij gebruik van het netwerk van een derde, deze blokkeringsmogelijkheid aan moet bieden, de aanbieder van het (onderliggende) netwerk of de aanbieder van de telefoondienst dan wel de carrierdienst.

8.2. Uitvoeringsaspecten

De sector geeft hier een antwoord in lijn met vraag 6 over de toedeling van verantwoordelijkheden. Sommige vinden dat de aanbieder van de carrierdienst de blokkeringen moet aanbieden en dat de aanbieder van het onderliggende netwerk de blokkeringen moet uitvoeren. De C(P)S-aanbieder moet deze mogelijkheid aanbieden, omdat hij de telefoondienst aanbiedt. Indien hij beschikt over de technische mogelijkheden kan de C(P)S aanbieder wellicht zelf de technische uitvoering verzorgen. Een andere optie is dat hij ervoor zorgt dat de netwerkaanbieder de permanente blokkering realiseert.

Een deel van de sector stelt dat in het nieuwe regelgevend kader de verplichting tot nummerblokkering is opgenomen in artikel 10, tweede lid, van de Universeledienstrichtlijn 2002/22/EG[8], hetgeen met zich meebrengt dat alleen de UD-aanbieders verplicht zullen zijn om nummerblokkering aan te bieden. Deze opvatting is inmiddels door nieuwe regelgeving achterhaald, daar, indien de eindgebruiker een consument is, ook C(P)S-aanbieders de dienst nummeridentificatie moeten aanbieden (artikel 3.3. RUDE), behoudens gevallen genoemd in artikel 3.3., vijfde lid, RUDE.

De sector brengt verder de zienswijze naar voren dat de vraag bij welke aanbieder de permanente blokkering moet worden *aangevraagd* een andere is dan de vraag welke aanbieder de permanente blokkeringsmogelijkheid zou moeten *bieden*. Gesteld werd dat een abonnee er voor kan kiezen om verschillende categorieën gesprekken (vast-mobiel, lokaal etc.) via verschillende C(P)S-aanbieders te laten lopen of zelfs om per categorie een andere C(P)S-aanbieder te gebruiken. Abonnees kunnen echter ook meerdere of alle categorieën oproepen via één aanbieder laten lopen. Opgemerkt wordt dat het voor de abonnee ondoenlijk zal zijn om een permanente blokkering te moeten aanvragen bij meerdere C(P)S-aanbieders. Een centraal punt waar men dergelijke (blokkerings)voorkeuren kenbaar kan maken lijkt een bruikbaar alternatief. Dit vergt echter enige standaardisatie, hetgeen ook kosten met zich mee zal brengen.

8.3. Carrierdienstaanbieder is aanspreekpunt

Aanbieders van carrierdiensten zijn verplicht tot het bieden van de mogelijkheid van nummeridentificatie aan eindgebruikers (consumenten), tenzij dit technisch niet uitvoerbaar is of economisch onhaalbaar. Wanneer de aanbieder van de carrierdienst nummeridentificatie aanbiedt, dient hij volgens artikel 11.9 Tw ook de daaraan verbonden mogelijkheden tot blokkering te bieden. Als hij niet in staat is tot het aanbieden van nummeridentificatie, dan mag het nummer van de abonnee niet worden doorgegeven. Zonder waarborgen zoals die genoemd in artikel 11.9 Tw mag het nummer van de abonnee niet worden doorgegeven.

[8] Richtlijn 2002/22/EG van het EP en de Raad inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en –diensten (Universeledienstrichtlijn). De richtlijn regelt de beschikbaarheid van de universele dienst, hetgeen met zich meebrengt dat lidstaten ervoor moeten zorgen dat telecommunicatiediensten van een nader gespecificeerde kwaliteit en tegen een betaalbare prijs beschikbaar zijn voor alle eindgebruikers op hun grondgebied, onafhankelijk van de geografische locatie.

De C(PS)-aanbieder moet zorgdragen voor het aanbieden van een permanente blokkering. Kan hij dit niet zelf dan zal hij deze blokkering moeten regelen met de netwerkbeheerder. Voor de consument zal de C(P)S-aanbieder echter het aanspreekpunt blijven.

Het lijkt volgens enkele aanbieders onwenselijk dat een abonnee een aanvraag voor een permanente blokkering moet doen bij meerdere C(P)S-aanbieders. Het CBP ziet dit niet in. Immers, de consument hoeft bij het afsluiten van het contract met de C(P)S-aanbieder(s) slechts aan te geven dat zijn of haar nummer permanent geblokkeerd dient te worden. Dit ligt wellicht anders in het geval dat een consument contracten heeft afgesloten met meerdere C(P)S-aanbieders en op enig moment daarna besluit om het nummer permanent te laten blokkeren. Om in dat geval met alle C(P)S-aanbieders opnieuw afspraken te moeten maken kan als omslachtig worden ervaren.

De meest aangewezen weg om een permanente blokkering die betrekking heeft op meerdere C(P)S-aanbieders te regelen is volgens enkele aanbieders de instelling van een centraal punt (vergelijkbaar met het nummer 0800-1273 waar een abonnee zijn of haar voor C(P)S-instellingen kan wijzigen[9]) dan wel het indienen van een aanvraag bij de aanbieder van het onderliggende netwerk. Het CBP laat aan marktpartijen over hoe zij dit onderling willen regelen. Nog steeds moet daarbij in acht worden genomen dat voor de consument de C(P)S-aanbieder als verantwoordelijke geldt.

Merk op dat de oproepende partij in een situatie waarin een blokkering van een abonneelijn bestaat, niet op grond van de Tw aanspraak kan maken op de incidentele verstrekking van het oproepende nummer. Er is, met andere woorden, geen op de Tw gebaseerd recht om een permanente blokkering per gesprek te deblokkeren.

[9] 0800-1273 is het (gratis) nummer waar automatisch de preselectiecode voor C(P)S ingesteld kan worden, voor alle operators.

9. Grondslagen voor verstrekking

9.1. Inleiding

(vraag 8)
De consultatie ging onder meer in op de vraag of netwerkaanbieders zelfstandig bevoegd zijn tot het verstrekken van nummers in het kader van nummeridentificatie.

9.2. Overeenkomst abonnee-dienstaanbieder bepalend

De opvatting van het CBP dat de netwerkaanbieder in de regel niet zelfstandig bevoegd is tot verstrekking van nummers in het kader van nummeridentificatie wordt over het algemeen door de sector gedeeld. Bepalend dient te zijn wat de dienstaanbieder overeenkomt met zijn abonnees. De aanbieder van het netwerk kan niet zelf besluiten, maar dient de dienstaanbieder te volgen. Dit is naar het CBP meent in lijn met artikel 3.3 RUDE, waar bijvoorbeeld als uitgangspunt is genomen dat de netwerkaanbieder maatregelen moet treffen om onder meer aanbieders van carrierdiensten in staat te stellen hun verplichtingen ter zake van nummeridentificatie na te komen.
Bij deze opvatting werden ook kanttekeningen geplaatst. Terecht werd aangegeven dat in het kader van nummeridentificatie niet altijd kan worden gesproken van de verstrekking van een persoonsgegeven. Met name in de zakelijke markt, waar abonnees vooral bedrijven en vennootschappen zijn, zou de verstrekking van nummers niet steeds een grondslag behoeven te vinden in de WBP.
Enige respondenten meenden dat nummeridentificatie niet kan worden opgevat als een verstrekking van persoonsgegevens door een aanbieder, maar dat de eindgebruiker daarvoor zelf als verantwoordelijke moet worden aangemerkt. De aanbieder is in die opvatting de bewerker ten behoeve van de eindgebruiker. Deze benadering vindt naar het oordeel van het CBP geen steun in de wet. Het is de aanbieder en niet de eindgebruiker, die doel en middelen voor de verstrekking van nummers in het kader van nummeridentificatie vaststelt. De eindgebruiker kan dan ook niet worden aangemerkt als verantwoordelijke, in de zin van artikel 1, onder d WBP. Ook artikel 11.9 Tw, dat verplichtingen oplegt aan de aanbieder van nummeridentificatie, verdraagt zich niet met die opvatting.
Het CBP merkt in de regel de dienstaanbieder aan als de verantwoordelijke voor de verstrekking van persoonsgegevens in het kader van nummeridentificatie. De verantwoordelijkheid voor doorgifte berust niet bij de aanbieder van het onderliggende netwerk. De dienstaanbieder is primair verantwoordelijk voor het aanbieden van de dienst nummeridentificatie. De netwerkaanbieder faciliteert.

9.3. Grondslag voor verstrekking

De bevoegdheid tot verstrekking van persoonsgegevens door de dienstaanbieder dient te worden bepaald aan de hand van de WBP. In het consultatiedocument heeft het CBP aangegeven dat de grondslag voor verstrekking te vinden is in artikel 8, onder b WBP, dan wel in artikel 8, onder f WBP. In artikel 3.3 RUDE is aan aanbieders van openbare telefoonnetwerken of openbare telefoondiensten de verplichting opgelegd tot het aanbieden van nummeridentificatie als bedoeld in artikel 1.1, onderdeel cc, sub 1 Tw. Ook aanbieders van carrierdiensten zijn daartoe gehouden, op verzoek van consumenten. Voor de goede orde wijst het CBP erop dat hoewel de wet in genoemde gevallen vereist dat nummeridentificatie wordt aangeboden, er nog geen sprake is van een verstrekking van persoonsgegevens die noodzakelijk zou zijn om een wettelijke verplichting na te komen in de zin van artikel 8, onder c WBP. De regelgeving op basis van de Telecommunicatiewet verplicht slechts tot het aanbieden van nummeridentificatie met bijbehorende blokkeringsmogelijkheden en niet tot verstrekking van persoonsgegevens als

zodanig.[10] In artikel 8, onder c WBP kan derhalve geen grondslag worden gevonden voor de verstrekking van persoonsgegevens.
Sommigen meenden dat de grondslag voor verstrekking kan worden gevonden in 8, onder a WBP: de eindgebruiker kan nummeridentificatie naar behoeven uit en aanzetten en zou daarmee ondubbelzinnige toestemming geven voor de verstrekking van diens nummer aan de opgeroepene. Hiervoor heeft het CBP reeds aangegeven dat de eindgebruiker niet kan worden aangemerkt als verantwoordelijke voor de verstrekking. Zou dat wel zo zijn, dan zou dat als consequentie hebben dat de eindgebruiker zichzelf toestemming zou dienen te geven voor verstrekking. De opvatting dat de eindgebruiker zowel de verantwoordelijke zou zijn als degene die toestemming voor verstrekking zou geven is dan ook onjuist. Bovendien is van toestemming in de zin van artikel 8, onder a WBP alleen dan sprake als de aanbieder beschikt over een vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt (artikel 1, onder i WBP). Het nalaten van een blokkering kan niet worden opgevat als een dergelijke wilsuiting gericht op het verstrekken van een nummer. Dat zou bijvoorbeeld anders zijn als de gebruiker de mogelijkheid zou hebben om, door het intoetsen van een code, zelf actief het nummer te laten verstrekken aan de opgeroepene. Daarvan is evenwel geen sprake.
In de consultatie werd ook de opvatting naar voren gebracht dat de netwerkaanbieder de oproepen ten behoeve van de abonnee moet 'completeren'. De abonnee heeft daarvoor toestemming gegeven. In die zin zou ook de verstrekking van nummers in het kader van nummeridentificatie berusten op toestemming van de abonnee. Het CBP meent dat tot het completeren van een oproep niet steeds ook de verstrekking van het oproepende nummer aan het opgeroepen netwerkaansluitpunt behoort. Nummeridentificatie moet volgens het CBP worden beschouwd als een aparte faciliteit, die geen onlosmakelijk onderdeel vormt van de communicatiedienst. De instemming van de abonnee voor de te leveren telefoondienst omvat in die zin niet de nummeridentificatie. Artikel 8, onder a WBP biedt derhalve geen grondslag voor de verstrekking van nummers. Het CBP handhaaft dan ook het uitgangspunt dat de grondslag voor verstrekking in de regel te vinden is onder b en f van artikel 8 WBP.
Wat de grondslag van artikel 8, onder b WBP betreft is door een mobiele operator opgemerkt dat wanneer de abonnee er voor kiest om bepaalde gesprekken via een andere aanbieder te laten lopen, de verstrekking niet noodzakelijk is voor de uitvoering van de overeenkomst tussen de netwerkaanbieder en de abonnee. Het CBP kan zich daarin vinden. De overeenkomst tussen de aanbieder die de betreffende oproep verzorgt is bepalend.

9.4. Uitzonderingen

Het CBP vindt dat een netwerkaanbieder in de regel geen zelfstandige bevoegdheid heeft om los van de aanbieder van telefonie en in het kader van nummeridentificatie, nummers te verstrekken aan derden. Door meerdere respondenten is aangegeven dat in bepaalde gevallen toch een zelfstandige bevoegdheid voor de netwerkaanbieder kan bestaan tot verstrekking van nummers in het kader van nummeridentificatie, met name als het gaat om nakoming van een wettelijke verplichting. Genoemd werd de verstrekking van het oproepende nummer aan de alarmcentrales door netwerkaanbieders. Het CBP acht die opvatting juist. In het vernieuwde artikel 11.10, eerste lid, onder a Tw is de verplichting tot het verstrekken van het nummer van het oproepende netwerkaansluitpunt aan een alarmcentrale bij publieke diensten niet meer opgelegd aan de aanbieder van nummeridentificatie, maar zowel aan de aanbieder van een openbare elektronische communicatiedienst als aan de aanbieder van een openbaar elektronisch communicatienetwerk. De verstrekking van persoonsgegevens is als dan noodzakelijk om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is. Voor de verstrekking kan in dit geval in artikel 8, onder c WBP een grondslag gevonden worden.

Respondenten wezen op nog andere gevallen waarin de verstrekking van persoonsgegevens noodzakelijk zou zijn. De aanbieder van het netwerk zou nummers dienen te verstrekken aan

[10] de wettelijke verplichting tot het aanbieden van de dienst brengt, gelet op de blokkeringsmogelijkheden die de gebruiker heeft, niet per se de verstrekking van nummers met zich mee.

derden, waaronder de dienstenaanbieder of aan andere netwerkaanbieders, indien dit voor de levering van de dienst noodzakelijk is ten behoeve van routering, signalering, *billing* of andere uitvoeringszaken. De netwerkaanbieder moet ook kunnen optreden bij fraude of oneigenlijk gebruik van een dienst. Ook *malicious call tracing* en het optreden bij plaaggevallen werden in dit kader genoemd. Daarnaast moet de netwerkaanbieder voldoen aan een vordering van het OM op grond van het Wetboek van Strafvordering. Naar de opvatting van het CBP vallen de genoemde voorbeelden buiten het bestek van nummeridentificatie. Daarbij gaat het immers alleen om verstrekking van het oproepende nummer aan het opgeroepen netwerkaansluitpunt en niet om verstrekkingen in een ander kader. Om die reden kunnen de genoemde voorbeelden hier verder onbesproken blijven.

10. Doorschakelscenario's

10.1. Inleiding

(vraag 9)
Door het CBP is in het consultatiedocument gesteld dat in een aantal gevallen niet op voorhand duidelijk is wat de grondslag is voor de verstrekking van nummers in het kader van de dienst. Het CBP had daarbij onder meer het oog op doorschakelscenario's. Niet steeds is helder of het nummer van de bellende A, dan wel dat van B naar wie A doorgeschakeld heeft, wordt verstrekt aan de gebelde C. Daarmee samenhangende vragen kunnen niet worden beantwoord.

10.2. Mogelijkheden tot verbeterde transparantie

De CBP-vraag of er mogelijkheden zijn om in de sector afspraken over doorschakelscenario's te maken werd door het grootste deel van de respondenten niet met een eenvoudig 'ja' of 'nee' beantwoord. Uit de antwoorden komt het beeld naar voren dat die mogelijkheden wel aanwezig worden geacht, zij het dat de noodzaak daartoe vooralsnog ontbreekt. Aangegeven is dat eerst als de klanten dat belangrijk vinden dan wel als er sprake zou zijn van ernstige privacyschendingen, er binnen de sector tot nadere afspraken kan worden gekomen.
Een van de mobiele operators plaatste daarbij de kanttekening dat de internationale specificaties van ETSI bepalend zijn voor de standaardisatie van blokkeringsfaciliteiten. Een standaardisatie voor andere diensten dan spraak zal volgens deze respondent nog enige jaren vergen. Een andere aanbieder meent daarnaast dat het maken van afspraken binnen de sector door tegengestelde belangen niet mogelijk zal zijn.

Het CBP begrijpt uit de gegeven respons dat bij doorschakelen niet standaard het nummer van A dan wel dat van B wordt verstrekt. Een van de respondenten wijst in dit kader bijvoorbeeld op de mogelijkheid bij ISDN om twee nummers te presenteren, waarbij de aanbieder van de ontvangende partij zelfstandig kan bepalen welke nummers gepresenteerd worden. Na vluchtige beschouwing van enkele standaarden zoals bijvoorbeeld die voor ISDN ziet het CBP dat, indien er al voor verschillende situaties kan worden gekomen tot afspraken betreffende het te verstrekken nummer en de daarbij aan te bieden blokkeringsmogelijkheden, die afspraken in eerste instantie tot stand moeten worden gebracht op internationaal niveau.
Het CBP zal daartoe vooralsnog geen initiatieven nemen. In situaties van doorschakeling dient vooralsnog van geval tot geval te worden geoordeeld over de toepassing van de regels voor nummeridentificatie, uit de Telecommunicatiewet dan wel uit de WBP.

Over wie verantwoordelijk kan worden gehouden voor de dienst en het informeren van het publiek spraken slechts enkele respondenten zich uit. Volgens enige respondenten is de aanbieder van de oproepende telefoondienst verantwoordelijk voor het realiseren van keuzes van de oproepende gebruiker. In een van deze reacties werd aangegeven dat de 'originerende partij' waarop het oproepende netwerkaansluitpunt is aangesloten verantwoordelijk voor de naleving van de regels omtrent nummeridentificatie. Met andere partijen moeten afspraken worden gemaakt dat zij de nummeridentificatie-instellingen overnemen en niet wijzigen (*spoofen*) of niet doorgeven. Het CBP is van mening dat dit een goed uitgangspunt is. Andere opvattingen werden overigens niet naar voren gebracht.

Voor wat betreft het informeren van het publiek stelt het CBP zich op het volgende standpunt. De dienstaanbieder moet zijn oproepende abonnees in elk geval voor de meest voorkomende standaardsituaties van doorschakelen informeren over de regels die gehanteerd worden bij het verstrekken van nummers. Tot de meest voorkomende standaardsituaties rekent het CBP in elk geval het bellen naar een vast telefoonnummer dat is doorgeschakeld naar een netwerkaansluitpunt van een derde, dan wel naar het mobiele nummer van de betreffende opgeroepene. In dergelijke gevallen moet duidelijk zijn welk nummer aan de ontvanger van de oproep wordt doorgegeven en hoe de oproepende partij dat zou kunnen verhinderen.

11. Informatieverplichtingen

11.1. Inleiding

Het consultatiedocument werd door het CBP voorbereid op basis van onder meer de voor het publiek beschikbare informatie over nummeridentificatie bij telecommunicatieaanbieders. Naar het oordeel van het CBP schoot die informatie in zijn algemeenheid nog tekort.

Alvorens aan de bespreking van de vragen 10 tot en met 13 betreffende de informatieverplichtingen toe te komen zal het CBP nader uiteenzetten hoe de WBP en de Telecommunicatiewet zich in dezen tot elkaar verhouden.

11.2. Algemeen

Artikel 6 WBP bepaalt dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze dienen te worden verwerkt. Onder het begrip wet in dat artikel moet niet alleen de WBP worden verstaan, maar ook andere wetgeving inzake de verwerking van persoonsgegevens, zoals in dit geval hoofdstuk 11 van de Telecommunicatiewet. Het gaat hier blijkens de wetsgeschiedenis van de WBP om een schakelbepaling die verzekert dat de betrokken regelingen in onderling verband van toepassing zijn (Kamerstukken II, 25 892, nr. 3, blz 78). Voorwaarde voor een behoorlijke en zorgvuldige verwerking is, blijkens overweging 38 van Richtlijn 95/46/EG, dat de betrokkenen van het bestaan van de verwerkingen kennis kunnen hebben. Aldus is het informeren van betrokkenen mede bepalend voor de beoordeling van de vraag of een gegevensverwerking als rechtmatig kan worden aangemerkt.
De Telecommunicatiewet sluit de toepasselijkheid van de WBP niet uit. Blijkens artikel 11.2 Tw geldt voor aanbieders van openbare elektronische communicatienetwerken en –diensten een zorgplicht voor de bescherming van persoonsgegevens en de persoonlijke levenssfeer, onverminderd de WBP. Hoofdstuk 11 Tw bevat op onderdelen een aanvulling van de WBP, bijvoorbeeld bij het toekennen van rechten aan abonnees/rechtspersonen. In de meeste gevallen is er sprake van een nadere invulling. Volgens de wetsgeschiedenis van de Tw geeft hoofdstuk 11 op de sfeer van elektronische communicatie toegesneden en in voorkomend geval uitputtende normen, evenwel zonder van dat laatste voorbeelden te noemen (Kamerstukken II, 28 851, nr. 3, p. 45).

Om te bepalen over welke onderwerpen informatie verstrekt moet worden heeft het CBP in het consultatiedocument de algemene regeling in hoofdstuk 5 WBP als uitgangspunt genomen. Ingevolge artikel 33, tweede en derde lid WBP is de verantwoordelijke verplicht de betrokkene zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd mede te delen alsmede nadere informatie te verstrekken voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen. Blijkens de wetsgeschiedenis van de WBP dient de verantwoordelijke zich telkens af te vragen of deze omstandigheden met zich brengen dat verwacht mag worden dat de betrokkene een reëel belang heeft bij nadere informatie en zo ja, wat de omvang van deze informatie is (Kamerstukken II, nr. 3, p. 154).
In artikel 11.9, tweede lid, onder d Tw is bepaald dat bij ministeriële regeling nadere regels worden gesteld met betrekking tot de wijze waarop aanbieders gebruikers en abonnees voorlichten over het gebruik van nummeridentificatie. De RUDE geeft mede uitvoering aan artikel 11.9, tweede lid Tw. In artikel 4.5 RUDE is bepaald dat de aanbieder er zorg voor draagt dat voor eenieder op genoegzame wijze informatie beschikbaar is met betrekking tot nummeridentificatie, de daarbij geboden weigerings- en blokkeringsmogelijkheden van deze faciliteit, en de financiële aspecten daarvan. Een en ander onverminderd artikel 3.2 RUDE. In dit artikel is ten aanzien van aanbieders van openbare telefoondiensten de verplichting uitgewerkt tot het op genoegzame wijze bekend maken van informatie aan eindgebruikers over een aantal onderwerpen, zoals over de naam en het adres van de aanbieder, het aanbod van diensten en

daarvoor geldende tarieven en algemene voorwaarden en regelingen terzake van schadevergoeding, terugbetaling en geschillenbeslechting. Aanbieders van carrierdiensten dienen consumenten daarover genoegzaam te informeren.
Blijkens de toelichting strekt artikel 4.5 RUDE tot implementatie van artikel 8, zesde lid van Richtlijn 2002/58/EG. Daarin is bepaald dat het publiek dient te worden geïnformeerd over het aanbod van nummeridentificatie alsmede over de blokkeringsmogelijkheden. Wanneer informatie op genoegzame wijze is bekendgemaakt is toegelicht in paragraaf 3 van het algemene deel van de toelichting op de RUDE. Samengevat komt het er op neer dat de informatie laagdrempelig toegankelijk moet zijn voor eindgebruikers. Daaraan wordt voldaan als de informatie op schrift wordt gesteld en aan de abonnees ter hand wordt gesteld. Aan potentiële abonnees moet de informatie op verzoek worden verstrekt. Het enkel informeren door middel van een website is niet toereikend: voor eindgebruikers die niet beschikken over toegang tot het internet dient een andere laagdrempelige verspreidingsvorm beschikbaar te zijn.

11.3. Informatieverplichtingen buiten de Tw

Een van de respondenten heeft vraagtekens geplaatst bij de bevoegdheid van het CBP om verdergaande eisen te stellen aan nummeridentificatie dan de Telecommunicatiewet stelt. De Telecommunicatiewet zou als specifieke regeling voorgaan op de WBP. Daarnaast werd gesteld dat de Tw een passend beschermingsniveau voor nummeridentificatie biedt en ook de mogelijkheid kent tot het stellen van nadere regels terzake van de informatieverplichtingen. Volgens het CBP komt deze benadering er op neer dat artikel 11.9 Tw een uitputtende regeling zou geven waar het de verstrekking van informatie over nummeridentificatie betreft. In dat geval zou de WBP als algemene regeling verder buiten toepassing dienen te blijven.
Het CBP stelt echter vast dat de tekst van artikel 11.9 Tw, noch de wetsgeschiedenis, noch de uitvoeringsregelingen aanwijzingen geven dat de toepasselijkheid van de WBP waar het de informatieverplichtingen betreft zouden zijn uitgesloten.
Naar de opvatting van het CBP zou van een uitputtende regeling sprake zijn, als de eisen die de WBP stelt aan de informatieverstrekking aan de betrokkene volledig zouden zijn uitgewerkt in de Telecommunicatiewet. Ingevolge artikel 33, tweede en derde lid WBP is de verantwoordelijke verplicht de betrokkene zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd mede te delen alsmede nadere informatie te verstrekken voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen. De regels gesteld bij of krachtens artikel 11.9 Tw hebben betrekking op de wijze waarop de aanbieders gebruikers en abonnees moeten voorlichten over het gebruik van nummeridentificatie en meer in het bijzonder over het aanbod van nummeridentificatie alsmede over de blokkeringsmogelijkheden. Daarmee is, naar het CBP meent, weliswaar invulling gegeven aan de belangrijkste, maar niet aan álle aspecten van de informatieverplichtingen. Dit betekent dat de algemene informatieverplichtingen van de WBP naar het oordeel van het CBP onverkort van toepassing zijn voor die onderdelen die geen uitwerking hebben gekregen in of krachtens de Tw. Zo zien de informatieverplichtingen in de Tw bijvoorbeeld niet op de verplichte verstrekking van het oproepende nummer aan alarmcentrales. In dat geval zijn de bepalingen van de WBP van toepassing.
Met het bovenstaande is ook een antwoord gegeven op de door een respondent gestelde vraag of de wetgever heeft beoogd dat ook over uitzonderingssituaties informatie verstrekt moet worden.

12. Informeerverantwoordelijkheden bij carrierdiensten

12.1. Inleiding

(vraag 10)
Vraag 10 had betrekking op de verantwoordelijkheden voor het informeren in C(P)S-situaties of bij (ander) gebruik van een onderliggend netwerk van een derde. Naar de opvatting van het CBP was de beschikbare informatie in die situaties pover te noemen, onder meer omdat informatie over de identiteit van de verantwoordelijke doorgaans niet beschikbaar was. In een aantal gevallen werd eenvoudig doorverwezen naar de aanbieder van het onderliggende netwerk of naar andere informatiebronnen. Volgens het CBP dient de dienstenaanbieder zélf informatie beschikbaar te stellen, zodat duidelijk is hoe nummeridentificatie werkt en tot wie men zich moet wenden met vragen en opmerkingen over de dienst. De verantwoordelijkheid voor het informeren van abonnees en gebruikers kan niet zonder meer worden neergelegd bij de aanbieder van het onderliggende netwerk.

12.2. Toewijzing

De meerderheid van de respondenten zei zich te kunnen vinden in de visie van het CBP. De dienstenaanbieder dient zijn eigen eindgebruikers te informeren en de verantwoordelijkheid kan niet zonder meer bij aanbieder onderliggend netwerk worden gelegd. Volgens een respondent heeft de dienstenaanbieder een plicht te informeren over de wijze waarop persoonsgegevens worden verwerkt. De netwerkaanbieder zou daarop geen zicht (kunnen) hebben omdat dergelijke gegevens niet bij de netwerkaanbieder bekend (hoeven te) zijn.

Een respondent zei de CBP-visie dat de C(P)S aanbieder een eindverantwoordelijkheid heeft om nummerinformatie te faciliteren en daarover te informeren, niet te delen. De netwerkaanbieder is het aanspreekpunt voor het informeren van zijn eigen abonnees, dan wel ter uitvoering van interconnectie-afspraken met andere aanbieders. De informatieplicht volgt de klantrelatie, maar waar er technische onmogelijkheden zijn blijft de verantwoordelijkheid bij de netwerkaanbieder.

Andere respondenten zijn uitgegaan van een gezamenlijke verantwoordelijkheid. Een respondent stelde zich in de visie van het CBP te kunnen vinden, maar wees daarbij op de RUDE: de zorgplicht tot het beschikbaar zijn van informatie rust zowel op de dienstenaanbieder als op de aanbieder van het netwerk. Volgens die respondent dient ook een C(P)S-aanbieder daaraan te voldoen.
Een andere respondent meende dat in principe de dienstenaanbieder het aanspreekpunt dienst te zijn, maar dat het voor gewone vragen van operationele aard wenselijk kan zijn dat de klant terecht kan bij de onderliggende netwerkaanbieder. Volgens een andere respondent moet de netwerkaanbieder algemene informatie bestemd voor alle gebruikers beschikbaar stellen. De dienstenaanbieder dient de eigen abonnees te informeren. De netwerkaanbieder moet de dienstenaanbieder informeren over de dienst en over blokkeringen. Een respondent wees er in dit verband op dat er enkele gedragscodes tussen diverse partijen actief zijn, waarin is neergelegd hoe bepaalde informatie wordt verstrekt aan de klant.

Ten slotte wees een respondent op de samenhang met vraag 5: de informatieplicht uit hoofde van de WBP berust bij verantwoordelijke. Indien de dienstenaanbieder de verantwoordelijke is, moet die dus informeren. Het CBP kan zich hierin vinden. Zoals bij de bespreking van vraag 5 (zie hoofdstuk 7 Toedeling verantwoordelijkheden) is uiteen gezet, is het CBP van opvatting dat de aanbieder van C(P)S, als aanbieder van nummeridentificatie, ter zake van de door hem verzorgde communicatie gehouden is te voldoen aan artikel 11.9 Tw. Daarmee rusten op hem ook de informatieverplichtingen uit hoofde van de Tw. De C(P)S-aanbieder is tevens aan te merken als de verantwoordelijke voor de gegevensverstrekking in het kader van nummeridentificatie in de zin van de WBP, dus op hem rusten ook de verplichtingen uit hoofde van die wet. Voor een nadere onderbouwing wordt hier verwezen naar vraag 5.

Ook bij technische onmogelijkheden rust de verantwoordelijkheid jegens het te informeren publiek in de visie van het CBP niet bij de netwerkaanbieder. Deze heeft slechts een verantwoordelijkheid jegens de dienstenaanbieder.
Hoewel in de RUDE de zorgplicht tot het beschikbaar zijn van informatie ligt bij de aanbieder van het netwerk dan wel de dienstenaanbieders, stelt het CBP zich op het standpunt dat de dienstenaanbieder primair verantwoordelijk is en daarop kan worden aangesproken. Als de netwerkaanbieder te zijnen behoeve informatie aan het publiek beschikbaar stelt, dan heeft de dienstenaanbieder daarvoor in te staan. Dat geldt ook voor de beantwoording van vragen van operationele aard. Ook als de netwerkaanbieder dat op zich neemt, blijft de dienstenaanbieder daarvoor verantwoordelijk. Van een gezamenlijke verantwoordelijkheid jegens het publiek is naar de opvatting van het CBP geen sprake. De inhoud van gedragscodes op dit gebied is het CBP niet bekend. In de beschikbare informatie voor het publiek wordt daaraan, voor zover het CBP kan overzien, ook niet gerefereerd. Het CBP kan daarover derhalve geen uitspraken doen, anders dan dat in die gedragscodes rekening dient te worden gehouden met het hiervoor gestelde.

13. Beschikbaarheid informatie

13.1. Inleiding

(vraag 11)
Het CBP heeft in het consultatiedocument opmerkingen gemaakt over de over nummeridentificatie voorhanden zijnde informatie. Het had de indruk dat informatie in veel gevallen niet in voldoende mate beschikbaar en toegankelijk is. De sector is gevraagd hierop te reageren en om suggesties aan te dragen voor het optimaliseren van de informatieverstrekking.

13.2. Toegankelijkheidscriteria

Alle respondenten zeggen de opvatting van het CBP niet te delen. De aanbieders zouden er alles doen de klanten te informeren. De informatie werd toereikend geacht. Voor verbeteringen in de beschikbaarheid ziet geen van de respondenten aanleiding. Men ontvangt zeer weinig klachten over de dienst. De informatie is reeds naar behoefte en onduidelijkheden zijn niet gebleken. Een respondent wees er op dat de informatie op zijn website via meerdere zoekopties toegankelijk is. Een ander zegt prijzen te hebben ontvangen voor het beste contactcenter, wat in het algemeen iets zou zeggen over de beschikbaarheid en toegankelijkheid van informatie over de producten en diensten.
Als ingezette informatiekanalen werden genoemd de telefonische klantenservice, internetsites, de algemene voorwaarden bij het aangaan van het contract, e-mail, een privacy statement op de website, de handleiding die klant ontvangt bij het afsluiten van een abonnement dan wel bij aankoop van een pre-paid kaart en die tevens on-line beschikbaar is, en een elektronisch doorkiesmenu waarmee de klant zelfstandig nummeridentificatie aan of uit kan zetten. De wachttijden bij klantenservice zouden in dat laatste geval geen probleem zijn.

Een respondent ging in het bijzonder in op de term ‘voldoende’ in artikel 5 van de inmiddels ingetrokken Regeling nummeridentificatie. De wijze waarop de informatie beschikbaar moet worden gemaakt is daaruit niet af te leiden. Deze respondent zag wel mogelijkheden tot verbetering door in de nieuwe ministeriële regeling de bekendmakingsverplichtingen meer aandacht te geven. Daarbij werd aangegeven dat internet, alsmede de algemene voorwaarden die bij het aanbieden van een dienst bekend moeten worden gemaakt, de meest geschikte media zijn.

Zoals hiervoor is uiteengezet dient de aanbieder van nummeridentificatie er zorg voor te dragen dat daarover voor een ieder op genoegzame wijze informatie beschikbaar is (artikel 4.5 RUDE). Dat laat onverlet de verplichting van artikel 3.2 RUDE voor aanbieders van openbare telefoondiensten tot het op genoegzame wijze bekend maken van informatie aan eindgebruikers over een aantal onderwerpen en voor aanbieders van carrierdiensten tot het genoegzaam informeren van consumenten daarover. Blijkens de toelichting RUDE (zie ‘§ 3. Eindgebruikersbelangen’) kan worden gesproken van het op genoegzame wijze informeren als de informatie laagdrempelig toegankelijk is. Daaraan wordt voldaan als de informatie op schrift wordt gesteld en aan de abonnees ter hand wordt gesteld. Aan potentiële abonnees moet de informatie op verzoek worden verstrekt. Het enkel informeren middels een website is niet toereikend: voor eindgebruikers die niet beschikken over toegang tot het internet dient een andere laagdrempelige verspreidingsvorm beschikbaar te zijn.
De WBP spreekt van het meedelen van informatie aan de betrokkene, tenzij deze daar reeds van op de hoogte is en wel uiterlijk op het moment van de eerste verstrekking (artikel 34, eerste lid WBP). Uitgangspunt is dat de informatie op zodanige wijze moet worden verstrekt, bijvoorbeeld schriftelijk dan wel elektronisch, dat de betrokkene daarover daadwerkelijk beschikt.

Naar het CBP veronderstelt heeft niet iedere respondent in zijn reactie rekening kunnen houden met de nieuwe regeling in de RUDE. De bekendmakingsverplichtingen zijn in de nieuwe RUDE duidelijker uitgewerkt dan in de oude regeling. Er geldt: de aanbieder die verantwoordelijk is

voor het aanbieden van nummeridentificatie is daarmee tevens verantwoordelijk voor het beschikbaar stellen van informatie.

Het CBP is er, anders dan de sector, niet van overtuigd dat de thans bij aanbieders voorhanden zijnde informatie in alle opzichten voldoet aan de hier genoemde eisen van beschikbaarheid en toegankelijkheid. Dit zal alleen van geval tot geval kunnen worden beoordeeld. Als vuistregel kan gelden dat aan eigen abonnees voorafgaand aan de verstrekking van hun telefoonnummer aan derden, op actieve wijze schriftelijk dan wel elektronisch informatie dient te worden verstrekt. Het aangaan van de overeenkomst is daarvoor een geschikt moment. Aan bestaande abonnees dient eveneens uit eigener beweging de benodigde informatie ter hand te worden gesteld. Die informatie moet tevens door een ieder op verzoek kunnen worden verkregen.
Als alleen algemene voorwaarden ter hand worden gesteld, geldt ook daarvoor de eis dat deze voldoende laagdrempelig toegankelijk dienen te zijn, wat in dat geval betekent dat ze voor een gemiddelde eindgebruiker begrijpelijk moeten zijn. Websites kunnen hier een aanvullende rol spelen, maar zijn als zodanig niet voldoende. Ook als informatie over nummeridentificatie via een website wordt verstrekt, zal die informatie voldoende toegankelijk dienen te zijn. Een telefonische informatiedienst zal eveneens de benodigde informatie moeten kunnen verstrekken en bovendien laagdrempelig toegankelijk dienen te zijn.

14. Inhoud informatie

14.1. Inleiding

(vraag 12)
Het CBP heeft de sector geconsulteerd over het aanvullen van de beschikbare informatie over nummeridentificatie, omdat aan sommige onderwerpen soms geen aandacht is besteed. De sector werd gevraagd naar redenen om de informatieverstrekking aan gebruikers niet aan te vullen.

14.2. Plaaggevallen en alarmdiensten

De sector is het niet eens met de constatering van het CBP dat de thans beschikbare informatie tekort schiet. Gesteld werd dat voorkomen moet worden dat de klant wordt overspoeld met informatie. De klant heeft behoefte aan korte en bondige informatie. Een respondent geeft aan geen redenen voor aanvulling te zien indien dat technisch en praktisch niet mogelijk is en indien het niet noodzakelijk is.
Uit het geringe aantal klachten wordt door de meeste respondenten afgeleid dat de huidige informatievoorziening toereikend is. Voor aanvulling ziet de sector geen aanleiding. Een respondent maakte onderscheid tussen het informeren van de eigen abonnees en het beschikbaar stellen van informatie aan een ieder. Volgens die respondent dienen abonnees in ieder geval compleet te worden geïnformeerd.

Het CBP ziet in dat het aantal klachten een indicatie kan zijn voor het maken van keuzes in de informatievoorziening. De sector gaat evenwel goeddeels voorbij aan de kwestie zelf, namelijk dat over een aantal onderwerpen kennelijk geen informatie voorhanden is, terwijl dat krachtens de wetgeving wel wordt vereist. De hierboven aangegeven redenen kunnen naar de opvatting van het CBP niet toereikend worden geacht om over de desbetreffende onderwerpen geen informatie aan te bieden.

Voor wat betreft de omvang van de informatieplicht heeft het CBP in het consultatiedocument de algemene regeling in hoofdstuk 5 WBP als uitgangspunt genomen. Ingevolge artikel 33, tweede en derde lid WBP is de verantwoordelijke verplicht om de betrokkene zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd mede te delen en om nadere informatie te verstrekken voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.
Op grond van de Telecommunicatiewet dienen aanbieders gebruikers en abonnees voor te lichten over het gebruik van nummeridentificatie en meer in het bijzonder over het aanbod van nummeridentificatie alsmede over de blokkeringsmogelijkheden.

Zoals hiervoor is gesteld wordt daarmee naar het CBP meent invulling gegeven aan de belangrijkste, maar niet aan alle aspecten van de algemene informatieverplichtingen. De algemene informatieverplichtingen uit hoofde van de WBP zijn dan ook onverkort van toepassing voor die onderdelen die geen uitwerking hebben gekregen krachtens de Tw.

Een respondent stelde dat het zeer de vraag is of de wetgever heeft beoogd dat ook uitzonderingssituaties bekend moeten worden gemaakt. Deze respondent betwijfelde of, waar het de verstrekking aan alarmnummers en plaaggevallen betreft, een uitbreiding van de informatieverstrekking afdwingbaar is, omdat de betreffende artikelen 11.10 en 11.11 van de Tw geen verplichtingen stellen ten aanzien van het bekendmaken van de gevolgen van deze verplichtingen aan gebruikers en abonnees.
Het CBP is, gelet op het hiervoor gestelde, een andere opvatting toegedaan. Op grond van de Telecommunicatiewet dient de informatie onder meer betrekking te hebben op de werking van nummeridentificatie, de daarbij geboden mogelijkheden tot blokkering van deze faciliteit en ook over de daarvoor gehanteerde algemene voorwaarden. Het CBP ziet niet in dat deze

verplichtingen niet zouden zien op gevallen waarin gekozen blokkeringen niet werken dan wel terzijde kunnen worden gesteld, zoals bij het optreden tegen telefoonhinder of bij het verzorgen van 112-oproepen. Als over deze situaties al niet krachtens de Telecommunicatiewet informatie beschikbaar dient te worden gesteld, moet worden nagegaan of artikel 33 WBP een verplichting met zich meebrengt daarover nadere informatie te verschaffen om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.
Het CBP overweegt als volgt. Omdat nummers in bepaalde gevallen door derden kunnen worden verkregen zonder dat de oproepende abonnee of gebruiker daarop invloed kan uitoefenen, moet voor hen ook informatie beschikbaar zijn over die gevallen, zodat zij daarop hun gedrag kunnen afstemmen. Het CBP meent derhalve dat ook over de onderwerpen nummeridentificatie bij plaaggevallen en bij alarmdiensten informatie beschikbaar dient te worden gesteld. Aan het ontbreken van expliciete informatie-opdrachten in de Tw komt dan ook geen beslissende betekenis toe.

15. Default bij geheime nummers

15.1. Inleiding

(vraag 13)
Het CBP heeft geconstateerd dat aanbieders als uitgangspositie de dienst nummeridentificatie inschakelen. Er is geen sprake van enige relatie tussen deze defaultinstelling en het hebben van een 'geheim nummer'. Zonder enige handeling van de abonnee zal diens nummer automatisch worden verstrekt aan derden.

Verschillende respondenten hebben aangegeven dat verhelderd zou dienen te worden wat moet worden verstaan onder een 'geheim nummer'. Het CBP is er in het consultatiedocument van uitgegaan dat deze term, althans in het normale spraakgebruik, voldoende duidelijk is. Voor de goede orde: het CBP heeft daarbij het oog op een nummer met bijbehorende naam-, adres- en woonplaatsgegevens van een abonnee, dat niet is opgenomen in een abonneelijst en / of een voor een abonnee-informatiedienst gebruikt abonneebestand. De respons op deze vraag heeft geen blijk gegeven van andere interpretaties van de term.

Volgens een mobiele aanbieder is deze discussie reeds gevoerd met OPTA en zou het CBP daarover met OPTA dienen af te stemmen. Zoals reeds in de begeleidingsbrief bij de consultatie is aangegeven, stemmen CBP en OPTA hun rolverdeling onderling af. Ook heeft OPTA deelgenomen aan de consultatie. De discussie waaraan is gerefereerd is nog niet naar voren gebracht. Hoe dan ook, gelet op de toepasselijkheid van de WBP waar het de informatieverplichtingen betreft, is er aanleiding om in te gaan op de defaultinstelling van nummeridentificatie.

Ook is naar voren gebracht dat het CBP zich eenzijdig zou richten op de privacy van de oproeper en te weinig op die van de opgeroepene. De laatste moet ook worden beschermd tegen spam, stalken, pesten en misbruik in het algemeen. Eveneens werd opgemerkt dat deze consultatie ook aandacht zou moeten besteden aan andere aspecten van nummeridentificatie, zoals *block blocking*. In de begeleidingsbrief bij het consultatiedocument is voor wat betreft de globale rolverdeling tussen OPTA en CBP voor nummeridentificatie genoemd dat OPTA toeziet op het aanbod van in de Telecommunicatiewet verplicht gestelde blokkeringsmogelijkheden, op kostenaspecten en op het gebruiksgemak, terwijl voor het CBP een taak is weggelegd met betrekking tot regels over het verstrekken van gegevens, het blokkeren daarvan en het informeren van de betrokkenen daarover. Het CBP heeft voorts in het consultatiedocument (zie alinea 7 in paragraaf 1.1.) aangegeven dat aspecten van nummeridentificatie die geen verband houden met de verwerking van persoonsgegevens in deze consultatie buiten beschouwing zijn gebleven, waarbij te denken valt aan bedieningsgemak, kosten, doorgifte van nummers aan netwerken die gekozen blokkeringen niet kunnen herkennen of block blocking.

Het merendeel van de respondenten is van opvatting dat er geen directe relatie is tussen het hebben van een 'geheim nummer' en nummeridentificatie. Het kiezen van een 'geheim nummer' brengt niet automatisch mee dat ook de nummeridentificatie standaard uit zou moeten worden gezet. Een van de aanbieders van mobiele telefonie heeft in dit kader aangevoerd dat het merendeel van de abonnees met een geheim nummer geen behoefte heeft aan permanente blokkering, om een aantal redenen. Door het nemen van een geheim nummer kunnen vooral willekeurige derden het telefoonnummer niet meer achterhalen via de telefoongids of nummerinformatiediensten. Via nummeridentificatie kan alleen de gebelde partij dat. 80% van de telefoongesprekken zou plaatsvinden tussen bekenden die het nummer al kennen. Ook zouden redenen van wederkerigheid hier een rol spelen: klanten met een geheim nummer zouden zelf ook graag zien wie hun belt. En de nummerverstrekking kan wel per gesprek worden geblokkeerd, maar een permanente blokkering kan niet per gesprek worden opgeheven. Ook volgens een andere mobiele aanbieder verdragen de huidige defaultinstelling voor

nummeridentificatie en het hebben van een geheim nummer zich goed. Gebruikers hebben daar geen moeite mee.
Het CBP kan zich vinden in de opvatting dat het hebben van een 'geheim nummer' niet direct impliceert dat nummeridentificatie standaard uit dient te worden gezet.

15.2. Defaultinstellingen

Geen enkele respondent ondersteunde de gedachte om de dienst nummeridentificatie standaard uit te schakelen bij abonnees met een 'geheim nummer'. Voor de gekozen defaultinstelling (standaard aan) zijn in de consultatie verschillende argumenten genoemd. Het standaard inschakelen zou in het belang zijn van de grootste groep eindgebruikers. Dat belang zou dienen te prevaleren boven het beperkte belang van een kleine groep gebruikers, zeker als die eenvoudig en kosteloos kunnen blokkeren. Anderen menen dat het recht om te zien wie er belt dient te prevaleren. De meeste mensen zouden wel herkenbaar willen zijn en zouden anders geen gebruik kunnen maken van bepaalde telefonische diensten.
Het CBP ziet geen basis in de wet om de dienst nummeridentificatie in het geval van abonnees met een geheim nummer standaard uit te zetten, dan wel eerst te activeren na een handeling van de abonnee zelf. Dat neemt niet weg dat de gekozen defaultinstelling aldus met zich meebrengt dat de aanbieders standaard ook 'geheime nummers' aan derden verstrekken, zonder dat de betreffende abonnee daarvoor zelf enige handeling dient te verrichten.

Verschillende respondenten hebben zich op het standpunt gesteld dat de betekenis van een 'geheim nummer' bij het aangaan van de overeenkomst duidelijk uiteen moet worden gezet. Door gerichte voorlichting aan de gebruiker, met name op moment dat deze aangeeft een nummer geheim te willen houden, waarbij deze wordt gewezen op de mogelijkheden om nummeridentificatie te blokkeren, zou er geen reden zijn daarnaast nog iets te doen. Voor bestaande abonnees zou voldoende informatie beschikbaar zijn over het aan- en uitzetten van de dienst.
Een aanbieder van mobiele telefonie gaf aan dat de keuze over de koppeling van een 'geheim nummer' en nummeridentificatie steeds bij de abonnee of gebruiker zelf zou moeten worden gelegd. Bij het aangaan van de overeenkomst zouden zij daarover duidelijk dienen te worden geïnformeerd.

Het CBP meent hierin een zekere steun te kunnen vinden voor een verbetering van de voorlichting, in elk geval aan nieuwe abonnees. Naar de ervaring van het CBP kunnen abonnees diverse belangen hebben om hun nummer niet vermeld te zien in een telefoongids of nummerinformatiedienst. Zo zijn er abonnees die belaagd worden door stalkers en om die redenen een 'geheim nummer' aanvragen. Anderen willen alleen bereikbaar zijn voor bepaalde personen. Gelet op de aard van een 'geheim nummer', is het CBP dan ook van oordeel dat hier een verplichting ingevolge artikel 33, tweede en derde lid WBP geldt voor de verantwoordelijke om de betrokkene nadere informatie te verstrekken. Bij het ontbreken van iedere informatie over de relatie tussen een 'geheim nummer' en nummeridentificatie kan, waar het het standaard inschakelen van nummeridentificatie betreft, niet meer worden gesproken van een behoorlijke en zorgvuldige verwerking van persoonsgegevens in de zin van artikel 6 WBP. Het CBP is al met al van oordeel dat door het geven van gerichte voorlichting bij het aangaan van de overeenkomst over de betekenis van een 'geheim nummer' waar het nummeridentificatie betreft, de standaard verstrekking van deze nummers rechtmatig doet zijn in de zin van de artikelen 6 jo 33, tweede en derde lid WBP.

16. Effectiviteit blokkeringen

16.1. Inleiding

(vragen 14 en 15)
Het CBP heeft de sector geconsulteerd over een aantal gevallen waarin de gebruiker geen reëel gebruik lijkt te kunnen maken van de aangeboden blokkeringsmogelijkheden. Aanbieders blijken soms alleen toegang tot bepaalde diensten te bieden op voorwaarde dat de nummerdoorgifte niet is geblokkeerd. Daarnaast heeft het CBP de sector de vraag voorgelegd in hoeverre het gerechtvaardigd is dat een ISP zich niet als eindgebruiker opstelt en nummers ontvangt ongeacht de ingestelde blokkeringen. De reacties op de vragen 14 en 15 bleken dicht bij elkaar te liggen. Om die reden worden beide vragen hier in samenhang behandeld.

Een respondent merkte in dit verband op dat de standaard voor nummeridentificatie alleen is neergelegd voor spraakdiensten; voor SMS of voor WAP zijn geen ETSI-specificaties neergelegd. Naar het CBP meent moet de reikwijdte van artikel 11.9 Tw dan wel van de WBP ook in dergelijke gevallen worden bepaald.

16.2. ISP's

Meerdere respondenten hebben zich op het standpunt gesteld dat ISP's moeten worden beschouwd als aanbieders van openbare telecommunicatiediensten. De uitwisseling van nummers zou in dat geval noodzakelijk zijn voor routering, facturering of andere zaken, zoals het tegengaan van misbruik. Dit zou los staan van nummerweergave in de zin van artikel 11.9 Tw. De ISP zou niet het eindpunt zijn van de communicatie en zou zich niet dienen op te stellen als eindgebruiker, maar als dienstverlener.
Een respondent stelde dat ISP's nummeridentificatie soms nodig hebben voor het afrekenen van telefoonverkeer met gebruikers: de ISP treedt dan tevens op als telefoondienstaanbieder voor wat betreft het inbellen. Bovendien is de ISP geen eindgebruiker, maar altijd een aanbieder van een communicatiedienst. Alleen als een ISP de telefoondienst voor het inbellen niet zelf afrekent met zijn klant zou de ISP ook kunnen worden beschouwd als een gebruiker in de zin van de Telecommunicatiewet.

Het CBP kan zich vinden in de opvatting dat een ISP zich niet steeds als eindgebruiker hoeft op te stellen, op grond van de volgende overwegingen. De oproepende abonnee dan wel gebruiker heeft het recht de verstrekking van zijn nummer aan het opgeroepen netwerkaansluitpunt te verhinderen. Of dat nummer mag worden verstrekt aan het netwerkaansluitpunt van de ISP, ongeacht de eventueel door de oproepende abonnee dan wel gebruiker gewenste blokkering, hangt af van het antwoord op de vraag of artikel 11.9, eerste lid onder a Tw op dit geval van toepassing is. Bepalend hiervoor is of het netwerkaansluitpunt van de ISP al dan niet kan worden aangemerkt als het opgeroepen netwerkaansluitpunt, als bedoeld in artikel 1.1, onder cc, sub 1 Tw.
Blijkens de definitie van netwerkaansluitpunt in artikel 1.1, onder k Tw gaat het om een fysiek punt waarop een abonnee toegang tot het netwerk wordt geboden. Indien er sprake is van een oproep gericht aan de aanbieder van een openbare telecommunicatiedienst teneinde van die aanbieder een andere telecommunicatiedienst af te nemen, kan er volgens het CBP niet worden gesproken van de verstrekking aan het opgeroepen netwerkaansluitpunt, maar van verstrekking aan een tussenliggend punt. Gelet hierop is er geen sprake van nummeridentificatie in de zin van artikel 1, onder cc Tw, wat ook maakt dat artikel 11.9 Tw geen toepassing vindt. Het CBP komt dan ook terug van zijn in het consultatiedocument geuite zienswijze dat in dit geval de keuze van de abonnee tot verhindering van de doorgifte van diens nummer de facto ter zijde wordt gesteld.

Door verschillende respondenten is aangevoerd dat het voor het leveren van bepaalde communicatiediensten eerst nodig is de identiteit vast te stellen aan de hand van het telefoonnummer van de eindgebruiker. Hierbij werden carrierdiensten genoemd waarbij

nummeridentificatie wordt gebruikt om te verifiëren of een gebruiker zich al dan niet heeft aangemeld. Een ander voorbeeld betreft faciliteiten zoals een terugbelvoorziening, die niet kan functioneren als de nummeridentificatie is geblokkeerd.
Omdat in beide voorbeelden de verstrekking niet plaatsvindt aan het bij de dienst behorende (opgeroepen) netwerkaansluitpunt, maar aan een tussenliggend punt, meent het CBP dat de regels van artikel 11.9 Tw niet van toepassing zijn op dergelijke verstrekkingen.

Dat ligt volgens het CBP anders bij oproepen die gericht zijn aan de aanbieder van een openbare telecommunicatiedienst, waarbij de oproeper het oogmerk heeft van die aanbieder een andere dienst dan een telecommunicatiedienst af te nemen. In dat geval is sprake van verstrekking aan het opgeroepen netwerkaansluitpunt en niet aan een tussenliggend punt: de partij met wie je wilt communiceren wordt in dat geval direct bereikt. Een van de respondenten noemde in zijn reactie als voorbeeld een spaarprogramma waarbij deelnemers hun saldo kunnen opvragen bij een sprekende computer achter een 0800-nummer, waarbij zij aan de hand van nummeridentificatie worden geïdentificeerd.
Volgens het CBP geldt artikel 11.9 Tw in dat geval wél en dienen de door de oproepende partij gekozen blokkeringen te worden gerespecteerd. Volgens het CBP gaat hetzelfde op bij andere door de sector genoemde voorbeelden, zoals oproepen die gericht zijn op het opwaarderen van prepaidkaarten of het bankieren via de mobiele telefoon. Het honoreren van de gekozen blokkeringen kan dan impliceren dat bepaalde toegevoegdewaardediensten niet bereikbaar zijn. Daarover dient de aanbieder zijn klanten ingevolge de WBP te informeren.

16.3. Toegevoegdewaardediensten

Over de toepasselijkheid van artikel 11.9 Tw bij het leveren van toegevoegdewaardediensten met een gemengd karakter (deels telecommunicatiedienst, deels anders) zal van geval tot geval moeten worden geoordeeld.
Het CBP zal zich in dergelijke gevallen conformeren aan het oordeel van OPTA of er al dan niet sprake is van een verstrekking aan een opgeroepen netwerkaansluitpunt. Als daarvan sprake is dan zal de aanbieder de gekozen blokkeringen niet ter zijde mogen stellen.

De vraag of aanbieders van telecommunicatiediensten via nummeridentificatie verkregen nummers mogen vastleggen of gebruiken voor facturering van diensten zoals SMS en MMS, moet worden beantwoord op basis van artikel 11.5 Tw. Dat geldt ook voor het gebruik van nummeridentificatie voor het tegengaan van misbruik dan wel in het kader van controle van *wholesale*-rekeningen door aanbieders.

Strikt genomen biedt artikel 11.5 Tw niet steeds een rechtvaardiging voor een dergelijke vastlegging. In het door een respondent naar voren gebrachte voorbeeld van routering door een ISP is de nummeridentificatie alleen noodzakelijk bij het tot stand brengen van toegang. Voor het vervolgens routeren van uitgaand en inkomend internetverkeer is het vaste dan wel dynamische IP-adres voldoende en kan het middels nummeridentificatie verkregen nummer niet meer noodzakelijk worden geacht.

17. Samenvatting informatieplicht

17.1. Inleiding

In de hoofdstukken 11 tot en met 16 is de zienswijze van het CBP op de informatieplicht uiteengezet, soms in het kader van de bespreking van een ander onderwerp. Hieronder volgt een overzicht van de aspecten die voor het informeren relevant zijn

17.2. Algemeen

De in de Tw danwel RUDE gegeven regeling is niet uitputtend. In paragraaf 11.3 is gemotiveerd waarom ook de WBP een rol speelt bij het vaststellen van informatieverplichtingen.

17.3. Verantwoordelijke

De dienstenaanbieder, dat kan zijn de aanbieder van een carrierdienst, is verantwoordelijk voor de gegevensvertrekking in de zin van de WBP en daarmee ook voor het informeren. Deze zienswijze is een gevolg van de visie op de toedeling van verantwoordelijkheden, besproken in hoofdstuk 7. De uitwerking die toegesneden is op carrierdiensten is gegeven in hoofdstuk 12.

17.4. Beschikbaarheid, toegankelijkheid, middelen

In hoofdstuk 13 van dit document zijn regels gegeven aangaande de beschikbaarheid en toegankelijkheid van informatie. De algemene regeling in hoofdstuk 5 WBP leidt ertoe dat de verantwoordelijke ter waarborging van een behoorlijke en zorgvuldige verwerking informatie moet verschaffen over

- zijn identiteit;
- de doeleinden van de verwerking waarvoor de gegevens zijn bestemd;
- overige zaken, waaronder gevallen waarin gekozen blokkeringen niet werken dan wel terzijde kunnen worden gesteld, zoals bij het optreden tegen telefoonhinder of bij het verzorgen van 112-oproepen. Volgens het CBP betreft de informatieplicht ook de onderwerpen doorschakelscenario's en defaults bij 'geheime nummers'.

Verder dient duidelijk te zijn in welke gevallen het blokkeren van nummerverstrekkingen impliceert dat bepaalde toegevoegdewaardediensten niet bereikbaar zijn. Daarover dient de aanbieder zijn klanten ingevolge de WBP te informeren.

De nadere invulling in de Tw, waarbij geldt dat aan het ontbreken van expliciete informatie-opdrachten in de Tw geen beslissende betekenis toekomt, noemt verplichtingen tot informatieverstrekking over het gebruik van nummeridentificatie en meer in het bijzonder over het aanbod van nummeridentificatie alsmede over de blokkeringsmogelijkheden en over de daarvoor gehanteerde algemene voorwaarden.

Of voldaan is aan de hierboven genoemde informatieplichten moet van geval tot geval worden beoordeeld.

17.5. Overzicht van onderwerpen waarover informatie moet worden verstrekt

In onderstaande tabel is aangegeven over welke onderwerpen informatie beschikbaar moet worden gesteld, voor zover het onderwerpen betreft waarop het CBP zich als toezichthouder ziet.

nr	onderwerp	vereist volgens	toelichting in paragraaf.	opmerking
1	identiteit verantwoordelijke	art. 33 WBP en art. 3.2, eerste lid, onder a RUDE	7.2, 7.3, 12.2	
2	doeleinden van de verwerking	art. 33 WBP		

nr	onderwerp	vereist volgens	toelichting in paragraaf.	opmerking
3	werking nummeridentificatie	art. 4.5 RUDE	4.2	vgl. art. 33 WBP jo art. 6 WBP
4	weigeringsmogelijkheden	art. 4.5 RUDE		
5	blokkeringsmogelijkheden	art. 4.5 RUDE		
6	rolverdeling dienstenaanbieder netwerkaanbieder	art. 33 WBP jo art. 6 WBP	7.2, 7.3, 12.2	voor zover van toepassing
7	defaultinstelling	art. 33 WBP jo art. 6 WBP	15.2	i.h.b. voor houders van een geheim nummer
8	het niet-honoreren van blokkeringen	art. 33 WBP jo art. 6 WBP	16.2, 16.3	
9	consequenties blokkeringen	art. 33 WBP jo art. 6 WBP	16.3	i.h.b. bij toegevoegdewaarde-diensten
10	alarmdiensten	art. 33 WBP jo art. 6 WBP	14.2	
11	plaaggevallen	art. 33 WBP jo art. 6 WBP	14.2	
12	doorschakelscenario's	art. 33 WBP jo art. 6 WBP	10.2	

Een van de onderwerpen waarover wel informatie moet worden verstrekt, maar waarvoor het CBP niet als toezichthouder geldt betreft financiële aspecten, genoemd in artikelen 3.2 en 4.5 RUDE.

18. Bijlage 1 Enige kwantitatieve gegevens

18.1. Inleiding

In deze bijlage zijn enige kwantitatieve gegevens over de consultatie vermeld, zodat een indruk kan ontstaan over de gegeven respons. Bovendien kwamen er in de consultatie niet alleen inhoudelijke vragen aan de orde, maar ook enige die procedurele of redactionele aspecten betroffen. Ook daarover wordt in deze bijlage iets gezegd.

18.2. Aantallen

De consultatie richtte zich op een primaire doelgroep van 21 partijen, waaronder telecomoperators, branche-organisaties en de OPTA. Hieronder is aangegeven in welke mate deze partijen hebben gereageerd, verdeeld naar soort organisatie.[11]

		aantal aangeschrevenen	aantal respondenten	%
vast	zonder eigen netwerk	3	0	0
	met eigen netwerk	3	1	33
mobiel	zonder eigen netwerk	2	2	100
	met eigen netwerk	5	5	100
organisaties	van aanbieders	5	2	40
overige		3	1	33
	totaal	21	11	52

Alhoewel het ook andere partijen vrij stond mee te doen aan de consultatie zijn er geen reacties ontvangen anders dan uit de primaire doelgroep.

Gelet op de respons meent het CBP dat de reacties representatief zijn voor de denkbeelden van de sector.

18.3. Procedurele aspecten

Algemeen

In de uitnodigingsbrief bij de consultatie is aangegeven dat de consultatie de opmaat is tot het nader interpreteren van wet- en regelgeving voor de verwerking van persoonsgegevens in de telecommunicatiesector, rekening houdend met de uitvoeringspraktijk. De daarop volgende voorlichting geldt dan als voorloper van handhavingsactiviteiten. Omdat het CBP het voornemen heeft om ook voor andere onderwerpen te komen tot verduidelijking, was de consultatie over Nummeridentificatie niet alleen van belang in verband met de gedachtevorming rond inhoudelijke vragen, maar ook om te lering te trekken uit het consultatie*proces*.

Waardering

In het algemeen bestond er waardering voor het CBP-initiatief, zij het dat er ook kritische opmerkingen gemaakt zijn over de samenloop met het bij de Eerste Kamer in behandeling zijn van de nieuwe Telecomwet en over de toezichtsafbakening met OPTA. (Deze punten worden hieronder nader besproken.)

Juridisch kader

Uit opmerkingen van diverse respondenten bleek dat de onderlinge verhouding tussen de Tw, de WBP en andere regelgeving voortdurend aandacht verdient. Dit bracht voor het CBP de

[11] waar operators die afzonderlijk zijn aangeschreven mogelijk in een gezamenlijkheid hebben gereageerd is de volgende telwijze gehanteerd. Indien voor het CBP herkenbaar is dat zo een operator heeft gereageerd, dan telt hij als respondent, indien deze herkenbaarheid er niet is, dan telt de operator niet als zodanig. Er hebben dus mogelijk meer operators gereageerd dan voor het CBP zichtbaar is.

verplichting met zich mee om aan te geven op welke juridische uitgangspunten CBP-zienswijzen op nummeridentificatie zijn gebaseerd. Bij het geven van terugkoppeling is geprobeerd om zo nauwkeurig mogelijk aan te geven op grond van welke wet- of regelgeving CBP-interpretaties tot stand zijn gekomen.

Onderwerpkeuze
Het CBP heeft bij het ontwikkeling van het voorlichtingsinitiatief enige relevante thema's geselecteerd, waaronder Nummeridentificatie. De sector heeft aangegeven dat er onderwerpen zijn die een grotere actualiteit hebben, dan wel die ingaan op behoeften van gebruikers of abonnees. De door de sector voorgestelde onderwerpen Verkeersgegevens en Locatiegegevens zijn reeds door het CBP opgenomen in de lijst van voorlichtingsthema's.
Er kan nog niet worden aangegeven wanneer een nadere studie van deze onderwerpen in het kader van normontwikkeling aan de orde is.

Het onderwerp Spam geeft aanleiding tot een meer algemene positiebepaling van het CBP. Het is daarom niet zinvol om dit onderwerp in het kader van het voorlichtingsprogramma te behandelen.

Samenloop inwerkingtreding Tw
De door het CBP te geven zienswijze is gebaseerd op de nieuwe Tw. Verscheidene respondenten hebben nadrukkelijk gewezen op de omstandigheid dat de consultatie plaatsvond in een periode waarin de wijzigingsvoorstellen op de najaar 2003 bestaande telecommunicatiewet in behandeling waren bij de Eerste Kamer. De onzekerheid die samenhing met de inwerkingtreding van de telecomwet gaf aanleiding tot vragen over

- de verplichtstelling van de dienst nummeridentificatie;
- de reikwijdte van de Tw;
- en de totstandkoming van de lagere regelgeving;
- de toezichtsverdeling tussen OPTA en CBP.

Bij de inhoudelijke bespreking is het CBP ingegaan op de eerste drie onderwerpen. Het CBP heeft in paragraaf 3.4 al opgemerkt dat er bij het waarderen van de reacties rekening moet worden gehouden met de omstandigheid dat niet alle respondenten op de hoogte zullen zijn geweest van de regelgeving die in de RUDE is voorgesteld.
De toezichtsvraag, waarop in hoofdstuk 15 al kort is ingegaan, komt aan de orde in Bijlage 2.

18.4. Overige aspecten

Sommige respondenten hebben opmerkingen gemaakt over andere dan inhoudelijke aspecten van de consultatie. Deze opmerkingen zijn relevant, niet alleen vanwege het pilotkarakter van de consultatie, maar ook vanwege het belang van overlegefficiëntie.

De consultatie leidde tot de volgende inzichten.

- de thans gevolgde werkwijze is, ondanks de relatieve eenvoud van het onderwerp, zowel voor de sector als voor het CBP tijdrovend geweest;
- alhoewel het CBP grote zorg heeft besteed aan de redactie van de bij de consultatie betrokken documenten, zijn er in redactioneel opzicht nog enige verbeteringen denkbaar, niet alleen waar het gaat om het vergroten van de eenvoud van het beantwoordingsmodel, maar ook waar het gaat om een heldere presentatie van soms lastige items. Sommige respondenten wezen op het ongedefinieerde gebruik van het begrip 'geheim nummer'.

Aan bezwaren kan tegemoet worden gekomen door het opvoeren van redactionele kwaliteit en door te overwegen dat consultaties niet per se schriftelijk hoeven plaats te vinden.

19. Bijlage 2 Toezicht

19.1. Inleiding

Het CBP ziet toe op de verwerking van persoonsgegevens in het algemeen, waaronder de verwerkingen door telecommunicatieaanbieders. Het toezicht op de naleving van de Telecommunicatiewet, waaronder het hoofdstuk over de bescherming van persoonsgegevens en de persoonlijke levenssfeer, is opgedragen aan OPTA. Dit betekent dat er sprake is van een samenloop van toezicht, hetgeen noopt tot het maken van afspraken waaruit blijkt welke van de toezichthouders OPTA en het CBP voor onderwerpen de meest gerede toezichthouder is.
In het bijzonder moet duidelijk worden hoe de toezichtsverdeling tussen OPTA en het CBP luidt voor het onderwerp nummeridentificatie.

19.2. Toezichtsverdeling OPTA CBP

In de begeleidingsbrief bij het consultatiedocument is voor wat betreft de globale rolverdeling tussen OPTA en het CBP voor nummeridentificatie aangegeven dat OPTA toeziet op het aanbod van in de Telecommunicatiewet verplicht gestelde blokkeringsmogelijkheden, op kostenaspecten en op het gebruiksgemak, terwijl voor het CBP een taak is weggelegd met betrekking tot regels over het verstrekken van persoonsgegevens, het blokkeren daarvan en het informeren van de betrokkenen daarover. Het CBP heeft in het consultatiedocument (zie alinea 7 in paragraaf 1.1.) aangegeven dat aspecten van nummeridentificatie die geen verband houden met de verwerking van persoonsgegevens in deze consultatie buiten beschouwing zijn gebleven, waarbij te denken valt aan bedieningsgemak, kosten, doorgifte van nummers aan netwerken die gekozen blokkeringen niet kunnen herkennen of block blocking.

Op het moment van het samenstellen van dit document zijn er nog geen formele afspraken tussen OPTA en het CBP tot stand gekomen over de toezichtsverdeling bij aspecten van de dienst nummeridentificatie.
Het CBP zal, ongeacht de toezichtsactiviteiten van OPTA, toezien op naleving van regels over het verstrekken van persoonsgegevens, het blokkeren daarvan en het informeren van de betrokkenen daarover.