Subjectieve verwijtbaarheid

Een toets om de aansprakelijkheid van internettussenpersonen voor het faciliteren van auteursrechtinbreuken te beoordelen

Het internet opent de deur voor de wereldwijde uitwisseling en verspreiding van auteursrechtelijk beschermde werken. Grootste bedreiging voor de handhaving van auteursrechten op het internet vormen de zogenaamde 'peer-to-peer'-netwerken en BitTorrent-programma's, die voortdurend onder vuur liggen van de entertainment-industrie en aansprakelijk worden gesteld. Maar ook andere internetdienstverleners, zoals online marktplaatsen en zoekmachines, worden aangesproken voor hun betrokkenheid bij de online verspreiding van beschermde werken. In dit artikel wordt ingegaan op de vraag aan de hand van welke criteria kan worden vastgesteld of een internetdienstverlener onrechtmatig handelt en dus aansprakelijk kan worden gesteld voor het 'faciliteren van auteursrechtinbreuken'.

C.F.M. de Vries
Mr. C.F.M. de Vries studeerde informatierecht aan de Universiteit van Amsterdam en is sinds kort werkzaam als advocaat te Amsterdam. Dit artikel is een bewerking van de auteurs afstudeerscriptie aan de Universiteit van Amsterdam.

Inleiding

De komst van het internet heeft ingrijpende gevolgen gehad voor het auteursrecht. Populaire websites als Google en Wikipedia bieden toegang tot eindeloos veel informatie, waarvan een deel auteursrechtelijk beschermd is. YouTube maakt het voor een ieder mogelijk om filmpjes online te zetten. Via advertentieplatforms zoals Marktplaats en eBay kunnen gebruikers een veelheid aan producten verhandelen. Bovendien kan men met behulp van zogenaamde peer-to-peer- (P2P-)ruilnetwerken, BitTorrent-programma's of -nieuwsgroepen op Usenet, gemakkelijk muziek en films downloaden. Auteursrechthebbenden zien met lede ogen toe hoe hun werken buiten hen om op zeer grote schaal gekopieerd en verspreid worden. Het is, gelet op de grootschaligheid en de anonimiteit van de individuele inbreukmakers, niet vreemd dat in toenemende mate de websites en diensten die op het internet auteursrechtinbreuken 'faciliteren', in rechte worden aangesproken door auteursrechthebbenden.

Ook in de politiek staat het aanpakken van 'inbreukfaciliterende' internetdienstverleners hoog op de agenda, hetgeen onder meer blijkt uit de recente Speerpuntenbrief Auteursrecht van staatssecretaris van Veiligheid en Justitie Teeven. Teeven pleit onder meer voor een 'herbezinning op de thuiskopie-exceptie' (ofwel een downloadverbod) en het codificeren van 'de bestaande jurisprudentie die bepaalt dat websites en diensten die auteursrechtinbreuken faciliteren onrechtmatig handelen'.[1] Deze rechtspraak staat centraal in dit artikel. Door middel van een kritische analyse van de relevante Nederlandse jurisprudentie wordt bekeken onder welke omstandigheden en aan de hand van welke criteria een internetdienstverlener jegens de auteursrechthebbende(n) onrechtmatig handelt en dus – mits aan de overige voorwaarden[2] voor aansprakelijkheid op grond van onrechtmatige daad is voldaan – aansprakelijk kan worden gesteld voor het 'faciliteren van auteursrechtinbreuken'. Omdat rechthebbenden ook in Amerika al jarenlang strijd voeren tegen de ongeautoriseerde uitwisseling van auteursrechtelijk beschermde werken via het internet,[3] wordt ter vergelijking ook ingegaan op de

1 Brief van de staatssecretaris van Veiligheid en Justitie, 11 april 2011, Speerpuntenbrief Auteursrecht 20©20, speerpunt 3 . Zie ook Teeven's reactie op vragen naar aanleiding van deze Speerpuntenbrief, te vinden op http://www.boek9.nl/files/2011/artikelen/Auteursrecht_Regering.pdf en de bijdragen van M.R.F. Senftleben en van J.N.T. Weda, J.P. Poort en I. Akker in *AMI* 2011/5. Of de door Teeven voorgestelde maatregelen er komen, is zeer de vraag. In december 2011 heeft de Tweede Kamer namelijk twee moties tegen het downloadverbod en websiteblokkades aangenomen omdat dergelijke maatregelen in strijd zijn met een vrij en open internet. Overigens heeft de rechtbank Den Haag zeer recent wel – op vordering van Stichting Brein – besloten dat internetproviders Ziggo en XS4ALL de downloadsite The Pirate Bay moeten blokkeren (Rb. Den Haag 11 januari 2011, *LJN* BV0549). Beide providers hebben inmiddels aangegeven in hoger beroep te gaan.

2 Namelijk: causaal verband, toerekenbaarheid, schade en relativiteit.

3 Dit blijkt onder meer uit de onlangs gelanceerde (en omstreden) wetsvoorstellen SOPA en PIPA. SOPA (de Stop Online Piracy Act) en zijn tegenhanger in de Amerikaanse senaat, PIPA (de Protect IP Act), zouden een zeer vergaande handhaving van auteursrechten online mogelijk maken, tot het (wereldwijd) blokkeren van websites aan toe. Om die reden is SOPA voorwerp van veel kritiek. Vele online diensten zouden immers door SOPA worden getroffen, hetgeen vergaande gevolgen heeft voor de informatievrijheid en een vrij en open internet. Op woensdag 18 januari 2012 gingen wereldwijd een aantal websites, waaronder Wikipedia, uit protest een dag op zwart. Deze kritiek heeft ertoe geleid dat beide wetsvoorstellen (voorlopig) van de baan zijn.

Amerikaanse rechtspraak over '*secondary liability*'. Duidelijk wordt, dat de criteria voor onrechtmatigheid (en dus aansprakelijkheid) in Nederland en in de Verenigde Staten niet essentieel van elkaar verschillen. Echter, bij een aantal van deze criteria zijn wel wat kritische noten op hun plaats. Bovendien ontbreekt een duidelijke en werkbare toets die internetdienstaanbieders vooraf duidelijkheid biedt en die als richtsnoer kan dienen in toekomstige zaken. In dit artikel zal ik een dergelijke toets formuleren.

De Nederlandse en Amerikaanse praktijk

Dat derden aansprakelijk kunnen zijn voor andermans auteursrechtinbreuken is zowel in de Verenigde Staten als in Nederland al jarenlang een algemeen aanvaard principe.[4] Het belang van een dergelijke 'indirecte' aansprakelijkheid – in de Verenigde Staten: secondary liability – heeft een enorme vlucht genomen sinds de opkomst van digitale peer-to-peer ruilnetwerken, waarmee op massale schaal auteursrechtelijk beschermde werken (wereldwijd) gekopieerd en verspreid worden.[5] Zowel in Nederland als in de Verenigde Staten heeft het '*peer-to-peer*-fenomeen' geleid tot een spectaculaire reeks rechtszaken, die zijn toegespitst op de vraag of de aanbieders van de onderliggende diensten en websites aansprakelijk zijn voor het faciliteren van de auteursrechtinbreuken gepleegd door hun gebruikers.

In beide landen wordt redelijk consequent aangenomen dat de aanbieders niet zelf (rechtstreeks) auteursrechtinbreuk plegen: dat doen immers de gebruikers. Uitzondering in dit verband was het *FTD*-vonnis van de voorzieningenrechter van de Rechtbank Den Haag,[6] waarin werd geoordeeld dat FTD (een forum met daarop informatie over bestanden op het Usenet[7]) auteursrechtinbreuk pleegde. Dit oordeel werd in hoger beroep echter resoluut teruggedraaid door het hof.[8] Meer recent, op 28 september 2011, werd door de Rechtbank Amsterdam echter wederom een verrassend vonnis gewezen. Geoordeeld werd dat Usenet service provider News-Server Europe zelfstanding inbreuk maakt op de auteursrechten van de bij Brein aangeslotenen.[9] Het is nog maar de vraag of dit vonnis in een eventueel hoger beroep standhoudt. De rechtbank gaat in dit vonnis namelijk voorbij aan alle eerdere uitspraken in vergelijkbare zaken, waarin de aansprakelijkheid consistent beoordeeld werd aan de hand van het leerstuk van de onrechtmatige daad, omdat het faciliteren an sich niet resulteert in een zelfstandige openbaarmaking of verveelvoudiging. Dit artikel gaat er daarom – conform vaste jurisprudentie – van uit dat een eventuele aansprakelijkheid gebaseerd moet worden op de onrechtmatigheid van het faciliteren van auteursrechtinbreuken. Aan de auteursrechtelijke grondslag voor aansprakelijkheid zal verder voorbij worden gegaan.

Nederland: Van *Kazaa* tot *FTD*

In Nederland wordt de aansprakelijkheid van inbreukfaciliterende websites en diensten gebaseerd op het leerstuk van de onrechtmatige daad (artikel 6:162 BW). Of het faciliteren van auteursrechtinbreuken onrechtmatig is, hangt af van de vraag of de 'faciliteerder' in strijd handelt met de in het maatschappelijk verkeer betamelijke zorgvuldigheid (de zorgvuldigheidsnorm). Op een ieder rust de verplichting om binnen zekere grenzen op te treden om de schade van derden te beperken of voorkomen. Hoe ver deze zorgplicht in een concreet geval strekt, is sterk casuïstisch bepaald, al wordt in de Nederlandse literatuur en rechtspraak wel een aantal algemene gezichtspunten die daarbij doorgaans een rol spelen onderscheiden.[10]

In de *Kazaa*-zaak[11] was van doorslaggevend belang of het file-sharing programma Kazaa ook geschikt was voor legitieme doeleinden, samen met de (on)mogelijkheid om

4 In de (vroegere) rechtspraak van beide landen zijn talloze voorbeelden te vinden van gevallen waarin werd geoordeeld dat anderen dan de primaire inbreukmakers – zoals uitgevers, kopieerwinkels en zaalverhuurders – aansprakelijk waren voor het faciliteren van auteursrechtinbreuken.

5 Met peer-to-peer programma's kunnen individuele gebruikers zelfstandig informatie aanbieden aan andere gebruikers ('peers'), dan wel informatie vinden en downloaden van deze andere gebruikers. De bestandsuitwisseling vindt direct plaats van de ene naar de andere gebruiker. Er zijn diverse soorten P2P-programma's. Sommige (de eerste generatie programma's) maken gebruik van een centrale server (zoals Napster), waarop verwijzingen naar bestanden op individuele computers worden opgeslagen en waarvoor tussenkomst van deze server vereist is voor de bestandsuitwisseling (de zogenaamde semi-gecentraliseerde programma's). Andere, latere programma's (zoals Kazaa) zijn decentraal en vervullen geen rol bij de daadwerkelijke bestandsuitwisseling, die kan plaatsvinden zonder enige controle en/of bemoeienis van derden. Een speciaal soort P2P-programma is BitTorrent, waarbij iedereen die een bestand downloadt dit bestand (automatisch) ook beschikbaar stelt (uploadt) voor andere gebruikers. Zie Chr.A. Alberdingk Thijm, 'Peer-to-peer vs. Auteursrecht', *Justitiële verkenningen*, jaargang 30, nr. 8, 2004 en B. Rietjens, 'Over *leechers*, *seeds* en *swarms*: auteursrechtelijke aspecten van BitTorrent', *AMI* 2006-1, p. 8-16.

6 Rb. 's-Gravenhage (Vzr.) 2 juni 2010, *IER* 2010, 20 (*FTD/Eyeworks*).

7 Het Usenet is een protocol waarmee via het internet bestanden kunnen worden verspreid. Usenet onderscheidt zich van P2P-uitwisselingsprogramma's als BitTorrent en eDonkey doordat de bestanden rechtstreeks gedownload worden van een centrale '*newsserver*', waardoor de downloadsnelheid vele malen hoger is dan bij andere peer-to-peer-netwerken. Nadeel van het Usenet is de onoverzichtelijkheid van de bestanden, die vaak vreemde namen hebben en daardoor moeilijk vindbaar zijn binnen het enorme aanbod op Usenet. FTD bood een dienst aan die voor dit probleem een oplossing biedt. FTD onderhield een forum waarop gebruikers zogenaamde 'spots' kunnen plaatsen. Een spot bevat informatie over een bepaald bestand, zoals de naam waaronder het bestand op Usenet is te vinden.

8 Hof 's-Gravenhage 15 november 2010, *IJN* BO3980 (*FTD/Eyeworks*).

9 Rb. Amsterdam 28 september 2011 (*BREIN/News-Service Europe*). De rechtbank gebiedt NSE om het vastleggen en aanbieden van zogenaamde 'binaries' (gecodeerde bestanden) te stoppen op straffe van een hoge dwangsom.

10 Zo is in het bekende *Kelderluik*-arrest (HR 5 november 1965, *NJ* 1966,136) een aantal richtsnoeren te vinden voor de beoordeling van onrechtmatig handelen. Van Dam heeft – voortbouwend op deze *Kelderluik*factoren – een aantal algemene gezichtspunten geformuleerd die meewegen bij de vraag of iemand onzorgvuldig handelt, namelijk: de aard en omvang van de schade, de waarschijnlijkheid dat deze schade zich zal voordoen, de aard van de gedraging en de bezwaarlijkheid van voorzorgsmaatregelen in termen van kosten, tijd en moeite (C.C. van Dam, *Zorgvuldigheidsnorm en aansprakelijkheid*, Deventer: Kluwer 1989, p. 110). In de zaak *Stokke/Marktplaats*, (Rb. Zwolle-Lelystad 14 maart 2007, *IER* 2007, 73) lijkt de rechter, in zijn uiteenzetting van factoren die van belang zijn bij het vaststellen van de zorgvuldigheidsverplichting van Marktplaats, deze factoren in het achterhoofd te hebben gehad (zie voetnoot 20).

11 HR 19 december 2003, *NJ* 2009, 548 (*Buma/KaZaA*) m.nt. P.B. Hugenholtz. *Kazaa* was de enige zaak waarin een peer-to-peer-programma direct zelf werd aangesproken, in plaats van een hulpdienst of verwijzende website. *Kazaa* is bovendien de enige uitspraak van de Hoge Raad waarin hij zich over dit onderwerp heeft uitgelaten, maar lijkt – gelet op de rechtspraak daarna – thans niet meer richtinggevend.

inbreukmakend handelen te voorkomen. Sinds de *Zoekmp3*-uitspraak[12] van het Hof Amsterdam lijken deze *Kazaa*-criteria echter permanent te zijn verlaten. Doorslaggevend voor de onrechtmatigheid in die zaak was het feit dat het businessmodel van zoekmachine Zoekmp3 gebaseerd was op het structureel inbreukmakend handelen door derden: het leeuwendeel van de bestanden waarnaar zij verwees was onrechtmatig, Zoekmp3 wist dit en profiteerde hiervan.[13] De *Zoekmp3*-criteria zien we in veel latere zaken terugkomen, zij het dat de focus niet altijd op hetzelfde criterium ligt. Zo werd ook in de *Shareconnector*-zaak geoordeeld dat sprake was van onrechtmatig handelen, met name omdat het doel van de website Shareconnector was om behulpzaam te zijn bij auteursrechtinbreuken (door uit het enorme aanbod van bestanden op het eDonkey peer-to-peer-netwerk nu juist die bestanden te selecteren die niet vervuild waren en de juiste inhoud hadden). Verder was de betrokken websitehouder bekend met het voor het leeuwendeel inbreukmakend handelen door de gebruikers en was hij hen structureel en systematisch behulpzaam daarbij.[14] In de bekende zaak tegen torrent-website Mininova[15] was het vooral de actieve rol en inhoudelijke bemoeienis van Mininova met de torrents op haar platform die leidde tot onrechtmatigheid. Mininova was haar gebruikers optimaal behulpzaam bij het uploaden van torrent-bestanden (die voor het grootste deel verwezen naar beschermde bestanden), stimuleerde het inbreukmakende handelen en profiteerde hiervan. Om dezelfde reden kwam de Rechtbank Amsterdam tot het oordeel dat het handelen van piratensite The Pirate Bay niet door de beugel kon.[16] Ook MyP2P handelde onrechtmatig, gelet op haar bekendheid met het feit dat via haar netwerk illegale content werd verspreid, haar (veronderstelde) intentie daarop, haar mate van betrokkenheid en de substantiële inkomsten uit de exploitatie van haar website.[17] In de recente procedures tegen FTD,[18] ten slotte, zien we alle eerder geformuleerde criteria terugkomen, maar wordt met name waarde toegekend aan het feit dat FTD er structureel en doelbewust aan bijdraagt dat uploaders hun doel beter bereiken.

Al met al komen de Nederlandse rechters in vrijwel alle gevallen[19] tot dezelfde conclusie (ja, er is sprake van onrechtmatig handelen), maar worstelen zij met de criteria om die conclusie te rechtvaardigen, waardoor het accent telkens op een ander criterium komt te liggen. Toch is er wel enigszins een coherente lijn waar te nemen. Met name de *Zoekmp3*-criteria hebben veel navolging gekregen en zijn later aangevuld met een meer feitelijke toets in *Mininova*: wat is de daadwerkelijke rol of bijdrage van de dienstaanbieder? Kijken we naar de Nederlandse jurisprudentie tot nu toe, dan kunnen we constateren dat de onrechtmatigheid van het faciliteren van auteursrechtinbreuken door internetdienstverleners doorgaans wordt beoordeeld aan de hand van een aantal terugkerende factoren. Het gaat om *kennis* (weet de dienstaanbieder, of behoort hij te weten, van het inbreukmakend handelen?), *profijt* (genereert hij inkomsten met het inbreukmakend handelen?) en de daadwerkelijke (actieve) *rol of betrokkenheid* van de aanbieder daarbij. Van belang is verder de *intentie* van de betrokken dienstverlener en de vraag of hij een (effectieve) '*notice-and-takedown*'-procedure (hierna: NTD of NTD-procedure) heeft ingevoerd.[20] Hierbij heeft te gelden dat naarmate de aanbieder dichter (actiever) bij de inbreuken van zijn gebruikers betrokken is, ook een zwaardere zorgplicht zal gelden (mogelijk zelfs een verplichting tot preventief filteren, zie het *Mininova*-vonnis), dan wanneer hij zich beperkt tot het louter verschaffen van de faciliteiten en zich verder niet inlaat met het inbreukmakend handelen van de gebruikers.

'Secondary liability' in de Verenigde Staten

In de Verenigde Staten worden – anders dan in Nederland – verschillende categorieën secondary liability (indirecte aansprakelijkheid) onderscheiden. Tot 2005 waren dat er twee: '*vicarious liability*' en '*contributory liability*'. Vicarious liability vereist dat een derde in staat is om controle uit te oefenen over de inbreukmakende activiteiten van een ander (maar dit nalaat) en daaruit bovendien (rechtstreeks) financieel voordeel haalt. Contributory liability is aan de orde als een derde met wetenschap van het inbreukmakende handelen door de primaire inbreukmaker, daaraan actief bijdraagt. Deze laatste vorm van aansprakelijkheid is in 1984 door het Supreme Court in verregaande mate beperkt. In het *Sony-Betamax* arrest,[21] waarin het ging om de vraag of Sony '*contributory infringement*' pleegde door het op de markt brengen van videorecorders waarmee de con-

12 Hof Amsterdam 15 juni 2006, *LJN* AX7579 (*Zoekmp3*).

13 In gelijke zin (en om dezelfde redenen) werd geoordeeld dat de websitehouder van Dutchtorrent onrechtmatig handelde. Zie Rb. 's-Gravenhage 5 januari 2007, *Computerrecht* 2007, 46 (*Brein/KPN*).

14 Rb. Amsterdam (Vzr.) 14 januari 2008, *IER* 2008, 61, later bevestigd in: Hof Amsterdam 16 maart 2010, *IER* 2010, 78 (*Shareconnector*). Deze uitspraak lijkt in vergaande mate aansluiting lijkt te zoeken bij de *Zoekmp3*-criteria. Echter, waar in *Zoekmp3* van doorslaggevend belang was dat met het faciliteren van inbreuken winst werd nagestreefd, was van een dergelijk winstoogmerk in deze zaak geen sprake. Hier ging het om een eenvoudige hobbyist (een student) die niettemin onrechtmatig handelde, omdat het zijn intentie was om systematisch en structureel het downloaden van illegale bestanden door zijn gebruikers te bevorderen.

15 Rb. Utrecht 26 augustus 2009, *IER* 2009, 60 (*Mininova*).

16 Rb. Amsterdam (Vzr.) 22 oktober 2009, *AMI* 2010,1 (*The Pirate Bay*).

17 Hof 's-Hertogenbosch 12 januari 2010, *IER* 2010 en Rb. 's-Gravenhage (Vzr.) 22 maart 2011 (*MyP2P*).

18 Rb. 's-Gravenhage beschikking van 11 mei 2010, Rb. 's-Gravenhage (Vzr.) 2 juni 2010, *IER* 2010, 80, Hof 's-Gravenhage 15 november 2010, *LJN* BO3980, Rb. Haarlem 9 februari 2011, *LJN* BP3757 (*FTD/Eyeworks*).

19 Uitzondering: *Kazaa* en *Marktplaats* (zie voetnoot 20).

20 Zie ook Rb. Zwolle-Lelystad 3 mei 2006, *IER* 2007, 73 m.nt. H. Struik (*Stokke/Marktplaats*), waarin de rechtbank grotendeels dezelfde criteria noemt bij het vaststellen van de zorgvuldigheidsplicht van Marktplaats. Onderwerp van dit geschil was de vraag of advertentieplatform Marktplaats onrechtmatig handelde door haar klanten de gelegenheid te geven inbreukmakende goederen te verhandelen. Naast de *bekendheid* met de schade, de *omvang* hiervan, de *rol* die de dienstverlener zelf speelt bij het inbreukmakende handelen, de vraag in hoeverre hij *profijt* trekt van het inbreukmakende handelen en de *genomen maatregelen* om handelend op te treden (zoals notice-and-takedown-procedures), is onder meer van belang of voor de *branche* en/of omgeving waarin het handelen plaatsvindt speciale regels gelden. Deze zaak is vergeleken met de rest enigszins een vreemde eend in de bijt, nu van het aanbieden van en/of behulpzaam zijn bij een filesharing-programma geen sprake was. Geoordeeld werd dat Marktplaats had voldaan aan haar zorgvuldigheidsverplichting.

21 *Sony Corp./Universal Studios, Inc.*, 464 U.S. 417, 456 (S. Ct. 1984).

sument auteursrechtinbreuk kon plegen, formuleerde het Supreme Court het '*substantial non-infringing uses*'-criterium: de aanbieder van een product of middel is niet aansprakelijk voor de daarmee gepleegde inbreuken, indien het middel ook geschikt is voor substantiële legitieme doeleinden. Deze '*safe harbor*' geldt niet indien de aanbieder daadwerkelijk kennis heeft van de inbreuken, maar deze kennis mag niet worden afgeleid louter uit de mogelijkheid dat het product geschikt is om daarmee inbreuk te maken. Ruim twintig jaar verschafte deze uitspraak de aanbieders van (nieuwe) technologieën een belangrijk schild tegen aansprakelijkheid.

Het *Sony*-criterium, tot stand gekomen in het tijdperk van de eerste kopieerapparaten en videorecorders, was evenwel niet voorbereid op de komst van digitale peer-to-peer filesharing netwerken en de daarmee gepleegde (wereldwijde) massa-inbreuken. Of en in hoeverre het *Sony*-verweer ook opgaat voor de aanbieders van dergelijke programma's – vast staat immers dat peer-to-peer-programma's, naast inbreukmakende gebruiksmogelijkheden, ook zeker geschikt zijn voor legitieme doeleinden – was onderwerp van discussie in de zaken tegen *Napster*[22] en *Aimster*.[23] In beide zaken werd het *Sony*-verweer uiteindelijk verworpen, zij het op verschillende gronden.

Napster kon niet aan contributory liability ontsnappen omdat zij – gelet op haar centrale (zoek)index – daadwerkelijke kennis had van de inbreuken door haar gebruikers, hieraan bijdroeg (door het beschikbaar stellen van de faciliteiten) en deze kon tegengaan. Diezelfde controlemogelijkheden, samen met het feit dat Napster's inkomsten afhankelijk waren van het aantal (inbreukmakende) gebruikers, bracht overigens mee dat ook was voldaan aan de voorwaarden voor vicarious liability.[24] Napster kon zich niet beroepen op *Sony* en stierf, ook als aanbieder van legale content, een langzame dood.

Ook peer-to-peer-netwerk Aimster kon zich niet verschuilen achter de geschiktheid van haar systeem voor legitiem gebruik. Anders dan het *Napster*-Court, oordeelt het 7th Circuit dat voor een geslaagd beroep op *Sony* op zijn minst moet worden aangetoond dat reeds sprake is van enig legaal gebruik (de enkele mogelijkheid van legitiem gebruik is niet voldoende), hetgeen bij Aimster niet het geval was. Bovendien is voor contributory liability volgens het 7th Circuit geen daadwerkelijke kennis vereist, maar volstaat '*general awareness*' alsmede '*wilfull blindness*'.

De tweede generatie peer-to-peer-netwerken (Grokster, Streamcast, Kazaa) trok lering uit Napster's ondergang. Nu een centrale zoekdatabank hun voorganger fataal was geworden, werden de opvolgende systemen volledig decentraal ontworpen, zodat de aanbieders geen kennis konden hebben van concrete inbreuken en daarover evenmin controle konden uitoefenen. De decentrale architectuur van deze programma's leek zijn vruchten af te werpen: Grokster en Streamcast konden zich bij de lagere rechters steeds met succes beroepen op het Sony-verweer, en gingen vrijuit voor zowel contributory als vicarious liability. Aan deze onaantastbaarheid van de decentrale peer-to-peer-netwerken maakte het Supreme Court in 2005 resoluut een einde met de belangrijke Grokster-uitspraak.[25] Het introduceerde een nieuwe (derde) onrechtmatigheidscategorie, '*inducement liability*', op basis waarvan een peer-to-peer-provider aansprakelijk is als wordt bewezen dat hij zijn programma aanbiedt met de intentie om inbreukmakend gebruik aan te moedigen, zelfs indien dat programma (ook) geschikt is voor legitieme doeleinden. De *Sony* safe harbor wordt uitdrukkelijk in stand gehouden, maar in die zin genuanceerd dat een aanbieder die de intentie heeft om inbreukmakend gebruik te bevorderen, zich niet kan verschuilen achter de substantial non-infringing uses van zijn programma. Een aantal factoren kan volgens het Supreme Court duiden op (kwade) intentie, waaronder het feit dat de aanbieder adverteert met de inbreukmakende gebruiksmogelijkheden, het feit dat zijn inkomsten afhankelijk zijn van inbreuken en de omstandigheid dat geen (effectieve) maatregelen zijn genomen om inbreuken te beperken.[26] In latere (lagere) Amerikaanse rechtspraak[27] worden bovendien ook kennis (van het grotendeels inbreukmakende karakter van de bestanden) en het feit dat de aanbieder zijn gebruikers behulpzaam is, aangemerkt als factoren die meewegen bij het vaststellen van een kwade intentie. Reeds hieruit blijkt dat de (criteria die gelden voor de) drie verschillende Amerikaanse doctrines elkaar in verregaande mate overlappen.[28] Zo zal het controlevereiste voor vicarious liability vaak ook een rol spelen bij het vaststellen van contributory liability en zal andersom vaak gelden dat het feit dat een dienstaanbieder materieel bijdraagt aan de inbreuken erop duidt dat hij daarover een '*right and ability to supervise*' heeft. Bovendien volgt uit de jurisprudentie dat met name de criteria

22 *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001). Napster was de eerste zaak waarin het Sony-verweer werd ingeroepen in de context van peer-to-peer-netwerken. Napster was het eerste P2P-programma en werd al snel ongekend populair. Na de rechtszaak tegen Napster volgde een reeks van zaken tegen andere aanbieders van filesharing programma's.

23 *In re Aimster Copyright Litigation*, 334 F.3d 643 (7th Cir. 2003).

24 De *Sony*-leer blijft hier overigens buiten beschouwing omdat deze alleen van toepassing is in de context van contributory infringement (in Sony was de vraag naar vicarious liability niet aan de orde). D.J.G. Visser, '"Napsterren", "Gnutellen" en de afwezigheid van legale muziek op het internet', *Computerrecht* 2001, p. 131.

25 *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 454 U.S. 125 (S. Ct. 2005).

26 De *Grokster*-uitspraak is van groot belang voor toekomstige zaken tegen aanbieders van peer-to-peer-netwerken en vergelijkbare diensten. Het Supreme Court geeft echter niet voldoende uitsluitsel over de vraag wanneer precies sprake is van inducement. Het signaleert enkel drie factoren die, in het specifieke geval van Grokster, relevant waren voor het vaststellen van een kwade intentie. Onduidelijk is bijvoorbeeld wat de gevolgen van de *Grokster*-uitspraak zullen zijn voor toekomstige programma's of software waar slechts een paar – of geen – van de *Grokster*-elementen aanwezig zijn, maar die desalniettemin op grote schaal inbreukmakend worden gebruikt.

27 *Arista Records LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124 (S.D.N.Y. June 30, 2009), *Arista Records LLC v. Lime Group LLC*, 2011 WL 1742029 (S.D.N.Y. May 02, 2011).

28 A.N. Dixon, 'Liability of users and third parties for copyright infringements on the Internet: overview of international developments', in: A. Strowel, *Peer-to-peer file sharing and secondary liability in copyright law*, Cheltenham: Edward Elgar Publishing Limited 2009, p. 35.

die gelden voor contributory liability (kennis, bijdrage) ook relevant zijn om inducement vast te stellen. Het komt mij voor dat het Supreme Court in *Grokster* bewust inducement als doorslaggevend criterium voor de aansprakelijkheid van peer-to-peer providers (en aanverwante dienstverleners) naar voren heeft willen schuiven en dat de oudere doctrines van contributory en vicarious liability daarmee minder relevant zijn geworden. Ook de oude situaties lijken immers 'gedekt' door de inducement-leer.

Toepasselijkheid van de safe harbors voor internet service providers

Zowel het Amerikaanse als het Nederlandse rechtsstelsel voorziet – in paragraaf 512 van de Digital Millennium Copyright Act (DMCA)[29] respectievelijk artikel 6:196c BW[30] – in een aantal wettelijke vrijwaringen van aansprakelijkheid voor bepaalde activiteiten van internettussenpersonen: '*mere conduit*',[31] '*caching*',[32] '*hosting*' en – alleen in de VS – '*information location tools*'.[33] Hosting, het op verzoek opslaan van de door een afnemer van de dienst verstrekte informatie, wordt in de praktijk door veel verschillende partijen verricht en is daarom juridisch het meest belangrijk.

De safe harbors uit de DMCA en artikel 6:196c BW fungeren als belangrijk 'filter' voor aansprakelijkheid (in Nederland voor alle vormen van aansprakelijkheid, in de Verenigde Staten alleen voor aansprakelijkheid in verband met inbreuken op het auteursrecht), want zij geven aan onder welke voorwaarden en omstandigheden een internetdienstverlener niet aansprakelijk is voor zijn aandeel in het ontsluiten van auteursrechtelijk beschermde (of in Nederland anderszins onwettige) informatie. Die voorwaarden zijn dat de internetdienstverlener geen daadwerkelijke kennis heeft van het onrechtmatige karakter van het materiaal en dit ook niet hoeft te hebben, en dat hij – zodra hij die kennis wel heeft – prompt handelt om de informatie te verwijderen of ontoegankelijk te maken (NTD).

Zowel in Nederland als in Amerika wordt in de rechtspraak redelijk consistent aangenomen dat de aanbieders van file-sharing diensten, torrentplatforms en index-sites geen beroep kunnen doen op de mere conduit- of hosting vrijwaringen. Beide regelingen kwamen tot stand in een periode waarin niet of onvoldoende rekening werd gehouden met het ontstaan van vele nieuwe soorten internetdienstverleners, waaronder de aanbieders van peer-to-peernetwerken. Verder zien we met name in Amerika dat de criteria van de DMCA en die voor contributory en vicarious liability op elkaar zijn afgestemd en elkaar uitsluiten.[34] In de Nederlandse rechtspraak wordt een beroep op artikel 6:196c BW (en de richtlijn Elektronische handel) steeds resoluut verworpen met de stelling dat de betreffende dienstverlener te 'actief' betrokken is bij de onrechtmatige informatie.[35]

Wel zien we dat de criteria uit het aansprakelijkheidsregime van de DMCA respectievelijk artikel 6:196c BW (en dan met name de criteria die gelden voor hosting providers) in sommige gevallen, zowel in Nederland als in de Verenigde Staten, als richtsnoer dienen bij het oordeel over de onrechtmatigheid.[36] Beide zijn immers bij uitstek regelingen die zijn toegespitst op en aanknopingspunten bieden voor de omvang van de verantwoordelijkheden en zorgplichten van tussenpersonen op het internet. Zo speelde, bij het oordeel over de onrechtmatigheid, in meerdere zaken een rol of de betreffende internetdienstverlener een (goedwerkende) NTD-procedure had ingevoerd.[37] Ook het kenniscriterium zien we in elke zaak terugkeren en is in

29 17 U.S.C. § 512.

30 Artikel 6:196c BW is een implementatie van de artikelen 12 tot en met 15 van de Europese richtlijn Elektronische handel (Richtlijn 2000/31/EG).

31 Bij mere conduit fungeert de dienstverlener in feite slechts als 'doorgeefluik'. Wanneer de dienst bestaat uit het louter doorgeven van informatie of het verschaffen van toegang tot een communicatienetwerk, dan is de dienstverlener niet aansprakelijk voor het eventuele onrechtmatige karakter van de doorgegeven informatie, mits hij op geen enkele wijze betrokken is bij de inhoud van de informatie en de dienstverlening een 'louter technisch, automatisch en passief karakter' heeft.

32 Onder caching vallen diensten die bestaan uit het automatisch, tussentijds en tijdelijk opslaan van van een ander afkomstige informatie.

33 Information location tools zijn bijvoorbeeld zoekmachines, hyperlinks en index-sites die verwijzen naar inbreukmakend materiaal.

34 M. Peguera, 'The DMCA Safe Harbors and Their European Counterparts: a Comparative Analysis of Some Common Problems', *Columbia Journal of Law & Arts* 2009-2, p. 481-512. '*The common-law requirements for contributory and vicarious liability are arguably codified in section 512 as elements that would disqualify a provider from the safe harbor.*'

35 Vgl. de *L'Oréal/eBay*-uitspraak van het Hof van Justitie van de Europese Unie (zaak C-324/09, 12 juli 2011). In deze zaak ging het (onder meer) om de vraag of online marktplaats eBay een beroep kon doen op de hosting-vrijwaring van de richtlijn Elektronische handel. Het Hof overweegt – anders dan AG Jääskinen in zijn conclusie – dat de beheerder van een elektronische marktplaats geen beroep kan doen op de vrijwaring als hij een 'actieve rol' heeft gehad. Van een dergelijke actieve rol is sprake als hij kennis van of controle over de gegevens heeft, of wanneer hij helpt bij het optimaliseren van de wijze waarop zij online worden getoond of bij de promotie van die aanbiedingen. In lijn met de eerdere *Google Adwords*-uitspraak (samengevoegde zaken C-236/08–C-238/08, 23 maart 2010) komt het Hof van Justitie aldus tot de conclusie dat een (internet)dienstverlener pas een beroep op de hosting-vrijwaring kan doen, als zijn rol in die zin neutraal is, dat zijn handelingen 'louter technisch, automatisch en passief' zijn.

36 Zie voor Nederland bijvoorbeeld *Stokke/Marktplaats* (Rb. Zwolle-Lelystad 14 maart 2007, *IER* 2007/73 m.nt. H. Struik) en voor de Verenigde Staten de zaak tegen YouTube: *Viacom International Inc./Youtube, Inc.*, 718 F. Supp. 2d 514 (S.D.N.Y. June 23, 2010). Vaststaat dat een (aanzienlijk) deel van de filmpjes op YouTube auteursrechtelijk beschermd is. Toch is YouTube niet aansprakelijk op grond van inducement liability, zo oordeelt het District Court, ondanks het feit dat YouTube in zijn algemeenheid op de hoogte is van het feit dat haar dienst door sommigen wordt gebruikt om inbreukmakende filmpjes te verspreiden en ondanks het feit dat YouTube's succes in ieder geval voor een deel gestoeld is op de aanwezigheid van inbreukmakend materiaal. Het District Court hecht veel waarde aan het feit dat YouTube aantoonbaar filmpjes verwijdert na daartoe strekkende notificaties van de rechthebbenden.

37 Marktplaats handelde niet onzorgvuldig, onder meer omdat zij een effectief notice-and-takedown-syteem had ontwikkeld. Mininova had weliswaar een NTD-procedure ontwikkeld, hetgeen meewoog bij de beoordeling, maar deze bood haar geen soelaas omdat de procedure niet voorzag in een effectieve methode voor het permanent verwijderen van inbreukmakende torrents. Ook omgekeerd geldt dat, wanneer een dienstverlener juist géén maatregelen treft, dit een omstandigheid is die meeweegt. De houding van The Pirate Bay, die openlijk NTD-verzoeken belachelijk maakte en bezwoer nooit een bestand te zullen verwijderen, was een belangrijke factor bij het oordeel over de onrechtmatigheid.

alle gevallen één van de voorwaarden voor onrechtmatigheid, met dien verstande dat aan het kennisvereiste buiten de safe harbors om al snel lijkt te zijn voldaan (kennis wordt vaak al aanwezig geacht als een dienstverlener in zijn algemeenheid weet dat de gebruikers inbreukmakend handelen), terwijl de DMCA en artikel 6:196c BW (en de richtlijn Elektronische handel) de drempel een stuk hoger leggen en daadwerkelijke kennis vereisen (welke pas bestaat na een uitdrukkelijke kennisgeving of in geval van onmiskenbaar onrechtmatige informatie[38]).

Gemeenschappelijke criteria

Ondanks grote verschillen tussen het '*common law*'-stelsel van de Verenigde Staten (het zogenaamde 'rechtersrecht') en ons '*civil law*'-stelsel, en de verschillende 'labels' en/of 'rubriceringen' – contributory, vicarious, en inducement liability of 'strijd met de maatschappelijke zorgvuldigheid' – die daar respectievelijk hier aan de aansprakelijkheid voor het faciliteren van auteursrechtinbreuken worden gegeven, wordt uit de praktijk duidelijk dat de benadering van de Amerikaanse rechter niet essentieel verschilt van die van de Nederlandse. Leggen we de relevante rechtspraak in Nederland en de Verenigde Staten naast elkaar, dan komt mijns inziens duidelijk een aantal gemeenschappelijke criteria naar voren die doorgaans – zowel in Nederland als in de Verenigde Staten[39] – worden toegepast bij het beoordelen van de vraag of een aanbieder van technologie onrechtmatig handelt. Het gaat om de volgende factoren:

- De *verhouding* tussen de faciliteerder en de primaire inbreukmaker: bevindt de dienstaanbieder zich in een dusdanige positie dat hij invloed kan uitoefenen op de inbreukmakende handelingen van de gebruiker(s)?
- De *mate van betrokkenheid* van de aanbieder bij de inbreuk: verschaft hij slechts de middelen of faciliteiten, of gaat zijn betrokkenheid bij de inbreukmakende handelingen verder dan dat?
- *Kennis*. Zowel in Nederland als in de Verenigde Staten lijken de rechters al snel kennis aan te nemen. De algemene wetenschap dat de gebruikers het programma (mede) gebruiken voor inbreuken wordt over het algemeen genoeg geacht.
- *Intentie gericht op het bevorderen van inbreuken*. Deze kan blijkens de rechtspraak worden afgeleid uit uitlatingen of andere gedragingen van de aanbieders, maar ook uit onverschilligheid of passiviteit (het niet nemen van maatregelen).
- De *mate* (het percentage) van het inbreukmakend gebruik: is het middel geschikt voor, dan wel zijn er (reeds) substantial non-infringing uses, of wordt het programma primair gebruikt voor inbreuken?
- *Profijt*. Het feit dat de (reclame)inkomsten van de aanbieder afhankelijk zijn van het aantal inbreukmakende gebruikers, is zowel in Nederland als in de Verenigde Staten een belangrijk criterium.
- De betrachte *mate van zorg* ('*due care*'). In het Nederlandse recht zit dit element 'ingebakken' in de onrechtmatigheidstoets, maar ook in de Verenigde Staten speelt het een rol. Heeft de aanbieder reeds maatregelen genomen om de auteursrechtinbreuken tegen te gaan? Hierbij wordt overigens wel rekening gehouden met de mogelijkheden die de betrokken aanbieder heeft[40] en met de *bezwaarlijkheid van maatregelen*. Bij dit laatste wordt, doorgaans aan de hand van een kosten-batenanalyse, onderzocht of het nemen van (preventieve) maatregelen van de aanbieder kan worden gevergd.[41]

Schiet een dienstverlener op twee of meer van de bovenstaande elementen tekort, dan zal dit – zo durf ik op grond van de besproken rechtspraak wel te concluderen – in de praktijk al snel leiden tot aansprakelijkheid. Sommige van de elementen (zoals kennis) zijn bovendien een essentiële voorwaarde voor aansprakelijkheid. De genoemde criteria zijn ontegenzeggelijk allemaal nuttig, maar bij (de toepassing van) een aantal zijn wel wat kritische noten op hun plaats. Ik noem er drie.

Criteria onder de loep

Allereerst het *kenniscriterium*. In alle besproken zaken speelde dit criterium een belangrijke rol. Dat kennis een *sine qua non* is voor (indirecte) aansprakelijkheid, is duidelijk en mijns inziens ook terecht. Iemand die geen wetenschap heeft van het inbreukmakend handelen van een ander, treft geen verwijt en behoort niet aansprakelijk te zijn.[42] Uit de rechtspraak wordt echter duidelijk dat de meeste rechters het feit dat dienstaanbieders *in abstracto*

38 Wanneer precies sprake is van 'onmiskenbaar onrechtmatig' materiaal, is niet geheel duidelijk. De memorie van toelichting noemt de situatie waarin een dienstverlener 'gegronde reden heeft te twijfelen aan de rechtmatigheid van de bij hem opgeslagen informatie in verband met de gerechtvaardigde belangen van derden'. *Kamerstukken II* 2001/02, nr. 3, p. 49. In de Amerikaanse DMCA bestaat een vergelijkbaar criterium, die wel wordt aangeduid als de '*red flag*'-test.

39 Maar ook in andere landen, zoals Australië, waar secondary liability de vorm aanneemt van '*authorisation*', spelen grotendeels dezelfde criteria een rol als die in het Nederlandse en Amerikaanse recht (A.N. Dixon, 'Liability of users and third parties for copyright infringements on the Internet: overview of international developments', in: A. Strowel, *Peer-to-peer file sharing and secondary liability in copyright law*, Cheltenham: Edward Elgar Publishing Limited 2009, p. 17).

40 De aanbieder van bijvoorbeeld videorecorders kan na het moment van verkoop geen invloed uitoefenen op wat de gebruikers er mee doen. Het aannemen van onrechtmatigheid ligt in zo'n situatie doorgaans niet of minder voor de hand. De aanbieders van P2P-netwerken, daarentegen, zullen over het algemeen meer zicht hebben op hetgeen de gebruikers op het netwerk doen en kunnen vaak (voor, tijdens, maar in ieder geval achteraf) optreden. Het bewust een 'oogje dichtknijpen' kan duiden op onvoldoende zorg.

41 A.N. Dixon, 'Liability of users and third parties for copyright infringements on the Internet: overview of international developments', in: A. Strowel, *Peer-to-peer file sharing and secondary liability in copyright law*, Cheltenham: Edward Elgar Publishing Limited 2009, p. 37-39.

42 Het kennisvereiste speelt in het Nederlandse aansprakelijkheidsrecht een rol bij de vraag naar de toerekenbaarheid. Voor toerekening van de onrechtmatige gedraging aan de dader op grond van schuld is (onder meer) vereist dat de schade of het risico voor hem 'kenbaar' was. In de Verenigde Staten is kennis eveneens een vereiste voor contributory liability. Voor vicarious liability geldt

weten dat hun dienst wordt gebruikt om inbreuk te maken, voldoende achten om kennis aan te nemen. Dat zij – mede door de architectuur van het systeem en/of het enorme aantal gebruikers – geen weet (kunnen) hebben van concrete inbreuken, doet hieraan niet af. Alhoewel ik het niet per se onlogisch vind dat de rechters kennis al snel aanwezig achten (inderdaad, tegenwoordig wéét iedereen dat via P2P-netwerken met name illegale bestanden worden uitgewisseld, dat Top 40-muziek en populaire films auteursrechtelijk beschermd zijn en dat de meeste torrent-bestanden verwijzen naar ongeautoriseerd materiaal), leidt een dusdanig ruime interpretatie van het kennisvereiste er mijns inziens wel toe dat dit criterium in belangrijke mate zijn relevantie verliest. In ieder geval kan de constatering dat sprake is van (algemene) kennis mijns inziens op zichzelf niet leiden tot onrechtmatigheid en volstaat een dergelijke kennis evenmin om er een kwade intentie uit af te leiden. Dit zou de mogelijkheid van (indirecte) aansprakelijkheid te ver oprekken. Wat zouden immers de gevolgen zijn voor diensten als e-mail, webwinkels (eBay, Marktplaats), iTunes, Google en YouTube? En voor de aanbieders of producenten van computerprogrammatuur, scanners en dvd-branders? Passen we het in de jurisprudentie gehanteerde kenniscriterium op hen toe, dan kunnen we concluderen dat al deze dienstverleners en aanbieders in zijn algemeenheid weten dat hun diensten respectievelijk producten ook (in aanzienlijke) mate inbreukmakend gebruikt kunnen en zullen worden. Toch is het onwenselijk om ze reeds daarom aansprakelijk te houden. Bestandsuitwisseling, ongeautoriseerde bestanden daaronder begrepen, is nu eenmaal de onmiskenbare realiteit van het internet. Daarom is algemene wetenschap naar mijn mening niet voldoende om onrechtmatigheid aan te nemen. Iets anders ligt het indien (aantoonbaar) sprake is van *daadwerkelijke kennis* van concrete inbreuken, bijvoorbeeld doordat de aanbieder of dienstverlener daarop uitdrukkelijk geattendeerd is. In zo'n geval zal de aanbieder of dienstverlener – naar analogie met de richtlijn Elektronische handel en de DMCA – onrechtmatig (moeten) handelen als hij nalaat om (prompt) de inbreukmakende bestanden te verwijderen.

Ook het *profijtcriterium* speelt zowel in de Nederlandse als de Amerikaanse rechtspraak in bijna alle gevallen een belangrijke rol bij het oordeel over de onrechtmatigheid. Het voeren van een business model dat (deels) afhankelijk is van inbreuken kan zelfs het doorslaggevende criterium zijn (vergelijk Zoekmp3) om aansprakelijkheid aan te nemen. Een zekere nuancering bij de toepassing van dit criterium is daarom wel op zijn plaats. Een middel dat zowel voor legitieme als niet-legitieme doeleinden kan wordt gebruikt, zal altijd door sommigen worden gebruikt om inbreuk te maken. In zekere zin wordt er daarom altijd meer verdiend door het inbreukmakend gebruik. Zou bewijs van profijt van inbreuk voldoende zijn, dan zou het aanbieden van kopieerdiensten of het verkopen van producten als iPods en harde schijven al (te) snel onrechtmatig zijn, hetgeen een afschrikkende werking kan hebben op de technologische ontwikkeling.[43] Om deze reden kan de constatering dat het business model van de aanbieder (deels) gebaseerd is op het inbreukmakend handelen van de gebruikers, mijns inziens op zichzelf niet doorslaggevend zijn bij het oordeel over de onrechtmatigheid. Profijt kan wel meewegen als indicator voor het vaststellen van een kwade intentie, of in samenspel met andere factoren tot onrechtmatigheid leiden. Daarbij moet echter niet voorbij worden gegaan aan de belangrijke vervolgvraag: hoeveel profijt? In de huidige rechtspraak wordt aan deze vraag doorgaans te weinig aandacht besteed. De enige situatie waarin het – naar mijn mening – gerechtvaardigd zou zijn om aansprakelijkheid louter te baseren op het profijtcriterium (waarbij ook de vraag naar de mate van het profijt irrelevant wordt), is wanneer een bepaalde technologie uitsluitend geschikt is voor inbreukmakend gebruik, hetgeen zelden of nooit het geval zal zijn.

Tot slot het substantial non-infringing uses-criterium. In Nederland speelt het beginsel – sinds *Kazaa*[44] – niet meer zo'n grote rol, maar in de Verenigde Staten is de vraag naar de juiste toepassing van het criterium onverminderd relevant. Veel technieken die geschikt zijn voor inbreukmakend gebruik, zijn bijna altijd ook inzetbaar voor legitieme doeleinden (zo ook P2P-netwerken en BitTorrent-programma's). De vraag of een middel 'geschikt' is voor (toekomstig) legitiem gebruik, is daarom niet erg van belang, nu het antwoord doorgaans bevestigend zal zijn. In hoeverre speelt dan het huidige legitieme (of juist inbreukmakende) gebruik een rol bij het oordeel over onrechtmatigheid? Welk gebruik (legaal of illegaal) de overhand zal hebben, is voor een technologie-aanbieder vooraf vaak moeilijk te voorspellen. Zou voor niet-aansprakelijkheid de voorwaarde gelden dat het middel aantoonbaar in substantiële mate rechtmatig gebruikt wordt (zoals het 7th Circuit in *Aimster* en de '*concurring opinion*' van Ginsburg bij *Grokster* wel betogen), dan bestaat het risico dat veel technologie-aanbieders het middel – uit voorzorg – maar niet op de markt brengen. Dit is onwenselijk. Het feit dat een programma of product voor het overgrote deel inbreukmakend gebruikt wordt, mag daarom op zichzelf niet tot aansprakelijkheid leiden. Deze omstandigheid kan wel worden meegewogen in combinatie met andere factoren, bijvoorbeeld voor het vaststellen van een kwade intentie. Andersom kan ook het tegenovergestelde – aantoonbaar en substantieel legaal gebruik – een omstandigheid zijn die meeweegt, dit keer in het voordeel van de aanbieder.

---

geen kennisvereiste omdat dit een vorm van risico-aansprakelijkheid is (traditioneel toegepast in de verhouding werkgever-werknemer) waarvoor geen verwijtbaarheid is vereist.

43 K.J. Koelman, 'MGM vs. Grokster – AKA Auteursrecht vs. Techniek', *Computerrecht* 2005-39, p. 4.

44 Het daar geformuleerde 'legitiem gebruik-criterium' doet denken aan de Amerikaanse '*substantial non-infringing uses*'-leer.

De noodzaak van een voorspelbare toets

De criteria zoals die nu in de Amerikaanse en Nederlandse rechtspraak worden toegepast, zijn allemaal relevant bij het beoordelen van de onrechtmatigheid van de handelwijze van internetdienstverleners. Zowel in Nederland als in de Verenigde Staten maken de rechters er echter in die zin een 'rommeltje' van, dat nu eens het ene en dan weer het andere criterium op de voorgrond treedt. Wat ontbreekt is een duidelijke en werkbare toets, die de uitkomst van toekomstige zaken tegen 'faciliteerders' van auteursrechtinbreuken voorspelbaar maakt. Toegegeven, de invulling van de ongeschreven zorgvuldigheidsnorm zoals neergelegd in artikel 6:162 BW ('strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt') is per definitie afhankelijk van de specifieke omstandigheden van het geval en dus 'onvoorspelbaar'. Desalniettemin bestaat er voor bepaalde situaties behoefte aan wat meer algemene regels. En de praktijk laat zien dat rechters inderdaad geneigd zijn bepaalde situaties (bijvoorbeeld gevaarzetting en sport- en spelsituaties) op een vergelijkbare manier te beoordelen. Naar mijn mening is het wenselijk dat ook de aansprakelijkheid voor het faciliteren van auteursrechtinbreuken nader geconcretiseerd wordt, althans dat een bepaalde toets als uitgangspunt genomen wordt bij de beoordeling van een concrete situatie.

Dat een dergelijke toets – die technologieaanbieders (zoveel mogelijk) *ex ante* duidelijkheid biedt – er komt, is van groot belang om de juiste balans te vinden tussen de bescherming van auteursrechten (ook op het internet) enerzijds en de vrije ontwikkeling van (communicatie)te chnologieën en de informatie- en communicatievrijheid anderzijds. Ook zijn met het wel of niet verbieden van technologieën vaak (grote) bedrijfs- en economische belangen gemoeid. Van belang is voorts het in het burgerlijk recht aanvaarde uitgangspunt dat derden in beginsel niet, maar slechts bij uitzondering, aansprakelijk (behoren te) zijn voor andermans onrechtmatige daad. Daarom moet worden gestreefd naar een methode die willekeur uitsluit en die de 'goede' internetdienstverleners (de aanbieders van nuttige technologieën die zich geconfronteerd zien met inbreukmakende gebruikers) afbakent van de 'slechte' (de technologie-aanbieders die actief bijdragen aan het inbreukmakend handelen van de gebruikers en/of dat beogen).[45]

Subjectieve verwijtbaarheid

Hiervoor (onder het kopje 'criteria onder de loep') is gebleken dat onrechtmatigheid in de huidige rechtspraak in veel gevallen uitsluitend of met name wordt beoordeeld aan de hand van objectieve aanknopingspunten, namelijk het feit dat het *leeuwendeel* van het gebruik inbreukmakend is, dat de dienstaanbieder hiervan *profiteert* en dat hij (algemene) *kennis*[46] heeft van de inbreuken. Aansprakelijkheid aannemen louter op basis van dergelijke geobjectiveerde elementen, is – op grond van de eerder aangevoerde redenen – mijns inziens echter niet wenselijk. Wil sprake zijn van een onrechtmatige daad, dan moet naar mijn mening ook enige 'subjectieve verwijtbaarheid' worden aangetoond. Subjectieve verwijtbaarheid – de bewoordingen suggereren het al – houdt in dat sprake moet zijn van subjectief (persoonlijk) verwijtbaar handelen. De reden dat onrechtmatigheid daartoe beperkt moet worden, is gelegen in de onwenselijkheid dat een aanbieder aansprakelijk kan worden gehouden op grond van omstandigheden die buiten zijn macht liggen.[47]

Als uitgangspunt voor de onrechtmatigheidstoets die ik in gedachte heb, neem ik een (internet)technologieaanbieder die (structureel) een product en/of dienst aanbiedt dat/die in *substantiële* mate (wellicht zelfs voor het *leeuwendeel*) gebruikt wordt voor *inbreukmakende* doeleinden, maar waarvan vaststaat dat het ook geschikt is (en gebruikt wordt) voor legaal gebruik. Bovendien ga ik ervan uit dat deze aanbieder in zijn *algemeenheid wetenschap* heeft van het feit dat zijn gebruikers het middel (ook) gebruiken om daarmee auteursrechtinbreuk te plegen. Laten we er bovendien van uitgaan dat hij – door middel van advertenties – *inkomsten* verwerft, die stijgen naarmate het aantal (inbreukmakende) gebruikers toeneemt. Duidelijk is dat bij deze aanbieder – die in de praktijk veel verschillende hoedanigheden kan aannemen, waaronder die van exploitant van een dienst als YouTube, Facebook, Wikipedia, Google, Dropbox, eBay, Skype, e-mail, een mp3-zoekmachine, een decentraal P2P-netwerk of een BitTorrent programma – de objectieve factoren, die in de Nederlandse en Amerikaanse rechtspraak van groot belang waren (algemene kennis, profijt, het grootste deel van het gebruik is inbreukmakend), aanwezig zijn.

Dat auteursrechthebbenden in de hier geschetste situatie een goede reden hebben om de desbetreffende aanbieder aan te spreken, is evident. Maar tegelijkertijd zal (vrijwel) iedereen het er over eens zijn dat niet alle van de hierboven genoemde aanbieders onrechtmatig handelen en aansprakelijk (zouden moeten) zijn. Immers, een groot deel van de online informatiediensten is wel geschikt voor het uitwisselen van beschermde werken en in die zin 'faciliteerder'. Er moet daarom een grens worden gesteld. Die grens ligt mijns inziens bij subjectieve verwijtbaarheid, waarvan sprake is in geval van het leveren van een *substantiële bijdrage* aan de auteursrechtinbreuken, het *aanmoedigen* van en/of aanzetten tot inbreuken, dan wel een combinatie van beide.

45 A.C. Yen, 'Third Party Copyright Liability After Grokster', 91 *Minnesota Law Review* 184 2006/2007, p. 224.

46 En dus niet specifieke kennis van concrete inbreuken.

47 K.J. Koelman, 'MGM vs. Grokster – AKA Auteursrecht vs. Techniek', *Computerrecht* 2005-39, p. 10.

Substantiële bijdrage

De eerste situatie waarin sprake is van subjectieve verwijtbaarheid, is die waarin de dienstverlener een *actieve, inhoudelijke bijdrage* levert aan het inbreukmakend handelen van zijn gebruikers. Om vast te stellen of daarvan sprake is, moet de rechter onderzoeken wat de daadwerkelijke *rol* van de dienstverlener is: hoe *substantieel* is zijn bijdrage en hoe *ver* verwijderd is het verband met de daadwerkelijke inbreuk? Hierbij dient vooropgesteld te worden dat het geven van (gebruikelijke) technische hulp of het leveren van (software)updates niet heeft te gelden als een substantiële bijdrage. Het geven van specifieke *instructies* voor illegaal uploaden, daarentegen, is dat wel, net als het *modereren* (bewerken) of het *selecteren* van illegale bestanden. In zo'n situatie handelt de aanbieder onrechtmatig, omdat hij inhoudelijk betrokken is bij de inbreukmakende bestanden. Dit geldt ongeacht de vraag of hij een NTD- of vergelijkbare procedure heeft ingevoerd (wat bij een dergelijke aanbieder doorgaans niet het geval zal zijn). In deze categorie vallen bijvoorbeeld Mininova, The Pirate Bay, Shareconnector en MyP2P, omdat zij allemaal inhoudelijk betrokken zijn (of waren) bij de gepleegde inbreuken door middel van moderatie (Mininova, The Pirate Bay) of selectie (Shareconnector en MyP2P) van de bestanden.

Aanmoediging

Een tweede scenario is dat waarin de aanbieder het inbreukmakende handelen van zijn gebruikers *actief aanmoedigt en/of stimuleert* (oftewel: inducement). In zo'n situatie ligt het aannemen van onrechtmatigheid voor de hand, zelfs als andere bijkomende omstandigheden – zoals profijt (Shareconnector) of verdere betrokkenheid – ontbreken, of als het middel maar in (zeer) beperkte mate inbreukmakend wordt gebruikt.[48] Dit is mijns inziens ook terecht, omdat het ten koste van anderen (de auteursrechthebbenden) aanmoedigen van inbreuken in strijd is met de maatschappelijke zorgvuldigheid.[49] Op deze grond zouden de aanbieders van het FTD-forum bijvoorbeeld aansprakelijk kunnen zijn. Weliswaar is er geen direct verband tussen de dienst die FTD verleent (het in stand houden van een forum voor berichten over bestanden op Usenet) en de uiteindelijke inbreuk, maar het doelbewust stimuleren van inbreuken door FTD zou desalniettemin aansprakelijkheid kunnen rechtvaardigen. Dat FTD haar gebruikers aanmoedigt, blijkt onder meer uit haar eigen mededelingen, de rol van haar moderatoren (hetgeen overigens ook leidt tot de vaststelling dat sprake is van een 'actieve bijdrage', zie hierboven) en het gehanteerde beloningssysteem. We hebben verder gezien dat ook de aanbieders van (decentrale) P2P-netwerken Streamcast en Grokster op deze grond aansprakelijk waren.

Het (op inbreuk gerichte) oogmerk van de aanbieder moet in beginsel duidelijk en ondubbelzinnig blijken uit externe[50] uitlatingen (expliciete aanmoediging) en/of handelingen van de aanbieder, alsmede uit de wijze waarop hij zich profileert[51] (impliciete aanmoediging), en mag niet worden afgeleid louter uit objectieve elementen (kennis, profijt, niet-filteren) of de architectuur van het programma of product. Van de aanbieder die ik hierboven als uitgangspunt nam voor de toets (hij weet in zijn algemeenheid van de grote hoeveelheid inbreuken en profiteert hiervan), kan dus nog niet – louter op basis daarvan – worden geconcludeerd dat hij de inbreuken stimuleert of aanmoedigt. Daarvoor is meer vereist, zoals stimulerende mededelingen (op de website), advertenties, of uit het (bewust) behulpzaam zijn van de gebruikers bij de inbreukmakende handelingen. In dit laatste geval is er een overlap met de hierboven geschetste categorie van 'actieve betrokkenheid'. De twee categorieën zullen overigens wel vaker hand in hand gaan, wat ook logisch is: een aanbieder die de intentie heeft om inbreukmakend gebruik te stimuleren, zal doorgaans ook (proberen om) een actieve bijdrage (te) leveren aan de inbreuken.

Substantiële bijdrage én aanmoediging

Dit brengt ons tot de derde – en laatste – situatie: die waarin de aanbieder *naast* een substantiële *bijdrage*, het inbreukmakend handelen *aanmoedigt* en/of stimuleert. In deze categorie vallen bijvoorbeeld The Pirate Bay en Mininova. Beide dienstverleners hebben (hadden) medewerkers (moderators) die zich actief bezighouden met de torrents en die torrents die verwijzen naar lege bestanden, kinderporno of virussen – maar niet: auteursrechtelijk beschermde werken – verwijderen. Daarnaast moedig(d)en beide dienstverleners hun gebruikers aan om meer torrents beschikbaar te stellen. Dit blijkt (naast de naam en het logo) bijvoorbeeld uit teksten op de website van The Pirate Bay, waaronder '*we are more determined than ever that what we do is right*' en '*seed those torrents a little bit more than you usually do*'. Het aanmoedigen van illegaal uploaden door Mininova bleek bijvoorbeeld uit het feit dat zij een speciale status toekende aan gewaardeerde uploaders.

48 A.N. Dixon, 'Liability of users and third parties for copyright infringements on the Internet: overview of international developments', in: A. Strowel, *Peer-to-peer file sharing and secondary liability in copyright law*, Cheltenham: Edward Elgar Publishing Limited 2009, p. 39-40.

49 A.C. Yen, 'Third Party Copyright Liability After Grokster', 91 *Minnesota Law Review* 184 2006/2007, p. 225-226. Zo kan alleen het voeren van de reclameslogan: 'waarom kopen, als je gratis kunt downloaden?' al reden zijn voor aansprakelijkheid. Enige uitzondering op deze hoofdregel zou zijn wanneer de aanmoediging geen enkel effect sorteert en niet resulteert in daadwerkelijke inbreuken (zonder primaire inbreukmaker kan immers ook geen afgeleide aansprakelijkheid bestaan).

50 In beginsel moeten de uitlatingen naar buiten, dus kenbaar voor het publiek, zijn gericht.

51 Zo profileert The Pirate Bay, met haar veelzeggende naam en piratenschiplogo, zich uitdrukkelijk als aanbieder van een dienst die inbreukmakend handelen mogelijk maakt en wil maken. Hieruit kan de intentie, gericht op het bevorderen van inbreuken, gemakkelijk worden afgeleid.

Géén actieve bijdrage of aanmoediging

Lastiger wordt het oordeel over de onrechtmatigheid wanneer de aanbieder in een wat verder verwijderd verband tot de daadwerkelijke inbreukmaker staat en er géén sprake is van een actieve bijdrage (alle hierboven genoemde aanbieders 'faciliteren' weliswaar op de een of andere manier inbreuken en leveren in die zin een bijdrage, maar niet allemaal bemoeien zij zich ook actief met de inhoud van de bestanden) of aanmoediging (de aanbieder onthoudt zich van mededelingen of gedragingen gericht op het bevorderen van inbreuken). In deze categorie vallen bijvoorbeeld webwinkels, (mp3-)zoekmachines en forumsites, die wel een rol spelen bij het vindbaar maken van inbreukmakende bestanden (bijvoorbeeld door middel van hyperlinks en/of categorisering en indexering), maar die niet rechtstreeks bijdragen aan het inbreukmakende handelen zelf. In zo'n situatie kan doorslaggevend zijn of de aanbieder enige effectieve maatregelen heeft getroffen om het aantal inbreuken te beperken of te voorkomen, zoals het invoeren van een NTD-procedure. Is dat het geval, dan handelt de aanbieder niet onrechtmatig. In deze categorie vallen bijvoorbeeld YouTube, eBay en Marktplaats, die alle voorzien in een effectieve NTD-procedure.[52]

Heeft de aanbieder echter geen NTD-procedure ingevoerd of vergelijkbare maatregelen getroffen, dan komt het (wederom) aan op de vraag hoe ver (of dichtbij) de technologieaanbieder af staat van de daadwerkelijke inbreuk. Is dat een (te) ver verwijderd verband, dan is het aannemen van onrechtmatigheid niet op zijn plaats. Dit geldt mijns inziens voor de aanbieders van diensten als Google en Zoekmp3. Ook zonder hun tussenkomst zijn de inbreukmakende bestanden immers beschikbaar en de zoekresultaten worden automatisch gegenereerd.[53] Staat een aanbieder wel dicht bij de inbreuk, maar weigert hij een NTD-procedure te implementeren, dan kan dit – naar analogie met de DMCA en de richtlijn Elektronische handel – resulteren in onrechtmatigheid (en aansprakelijkheid).

Deze situatie, waarin een actieve bijdrage en/of aanmoediging ontbreekt, is duidelijk de lastigste categorie. In deze categorie zullen ook (komen te) vallen de toekomstige decentrale P2P-netwerken die – net als het geval was na *Napster* – lering zullen trekken uit de *Grokster*-uitspraak en het in het vervolg wel zullen laten om het inbreukmakend handelen aan te moedigen of zich inhoudelijk met de inbreukmakende bestanden te bemoeien. In deze specifieke context kan mijns inziens echter niet voorbij worden gegaan aan de zogenaamde '*lineage*' van het programma: is een P2P-programma overduidelijk de 'opvolger' van zijn illegaal bevonden voorganger en richt hij zich op de gebruikers van dat andere P2P-netwerk (met dien verstande dat bewust de 'fouten' van die voorganger worden vermeden), dan mag een intentie gericht op het bevorderen van inbreuken naar mijn mening in beginsel worden verondersteld. Dit is een uitzondering op het uitgangspunt dat aansprakelijkheid in beginsel altijd moet volgen uit subjectief verwijtbaar gedrag maar deze lijkt me – in de context van P2P-programmatuur – terecht. Wil een dergelijke aanbieder vrijuit gaan, dan rust op hem de bewijslast om aan te tonen dat hij niet de intentie heeft gehad om in de voetsporen van zijn voorganger te treden. Dat kan hij doen door bijvoorbeeld aan te tonen dat '*good faith efforts*' zijn ondernomen om het aantal inbreuken effectief te bestrijden of terug te dringen.

In het schemergebied tussen rechtmatigheid en onrechtmatigheid, bevindt zich verder bijvoorbeeld de maker van de originele[54] BitTorrent software, alsmede de Usenet-provider. BitTorrent is de laatste generatie peer-to-peer-programmatuur en wordt op massale schaal gebruikt voor het uitwisselen van auteursrechtelijk beschermde werken. Aangenomen wordt dat de maker van BitTorrent (Bram Cohen) oorspronkelijk heeft willen voorzien in een middel voor de uitwisseling van Linux-software (die veelal vrij te verspreiden is) en niet in een product waarmee men inbreuk kan maken op intellectuele-eigendomsrechten.[55] Bovendien heeft Cohen onder meer deals gesloten met de MPAA (Motion Picture Association of America), teneinde het aantal auteursrechtinbreuken effectief terug te dringen.[56] Mocht BitTorrent in de toekomst door de muziek- en filmindustrie voor de rechter gedaagd worden, dan is niet uit te sluiten dat zij om deze reden vrijuit gaat.

Ook van het Usenet staat vast dat het oorspronkelijk ontwikkeld is als discussieforum voor uiteenlopende onderwerpen en niet als middel om daarmee op massale schaal inbreukmakende films en muziek uit te wisselen. Dat het Usenet zich in de loop der tijd wel in die richting ontwikkeld heeft, is de oorspronkelijke aanbieder niet aan te rekenen. Wel rust op Usenet-(ISP)providers de plicht om effectieve (NTD-)procedures in te voeren en/of andere maatregelen te treffen (met name met betrekking tot de

52 Op User-Generated Content platform YouTube kunnen individuele gebruikers filmpjes uploaden. Vaststaat dat een aanzienlijk deel van de video's op YouTube auteursrechtelijk beschermd is. Echter, YouTube bemoeit zich niet actief met de filmpjes, stimuleert het uploaden van illegaal materiaal niet en hanteert bovendien een streng NTD- *en* '*three strikes*'-regime. Dit laatste houdt in dat een individuele gebruiker die drie keer een inbreukmakend filmpje op YouTube zet, wordt geblokkeerd. Ook Marktplaats en eBay voorzien beide in een effectief Melding van Inbreuk-programma, waarmee rechthebbenden kunnen klagen over (inbreukmakende) advertenties.

53 Ook een forumsite als FTD zou in deze categorie vallen, ware het niet dat FTD inbreukmakend gebruik uitdrukkelijk lijkt aan te moedigen en dat aangetoond is dat een aanmerkelijk deel van de spotters ook uploader is, waardoor het verband tussen FTD en de daadwerkelijke inbreuk kleiner lijkt te worden.

54 En dus niet de vele diensten die, voortbouwend op het BitTorrent protocol, BitTorrent cliëntprogramma's of torrentwebsites hebben ontworpen en waarvan in veel gevallen een op inbreuk gerichte intentie aantoonbaar aanwezig is (denk aan The Pirate Bay).

55 Al gaan er ook geruchten rond dat uit een eerder manifest van Cohen zou blijken dat hij programma's ontwikkelde met het doel 'to commit digital piracy'. B. Rietjens, 'Over *leechers*, *seeds* en *swarms*: auteursrechtelijke aspecten van BitTorrent', *AMI* 2006/1, p. 16.

56 B. Rietjens, 'Over *leechers*, *seeds* en *swarms*: auteursrechtelijke aspecten van BitTorrent', *AMI* 2006/1, p. 15-16.

'verdachte' film- en muzieknieuwsgroepen). Dat de gespecialiseerde Usenet-providers (dus niet de internet service providers, maar die providers die Usenet als zelfstandige dienst aanbieden) onrechtmatig handelen, ligt eerder voor de hand, voor zover deze providers expliciet adverteren met het gemakkelijk uitwisselen van (recente) films en muziek (waardoor sprake is van inducement).[57]

Safe harbors

Uitgangspunt voor de hierboven uiteengezette toets is een (internet)dienst- of productaanbieder bij wie een aantal objectieve indicatoren voor onrechtmatigheid (algemene kennis, profijt en het feit dat de dienst of product in grote mate inbreukmakend wordt gebruikt) aanwezig zijn. Ik heb betoogd dat die objectieve aanknopingspunten niet doorslaggevend mogen zijn en dat deze aanbieder slechts onrechtmatig handelt als daarnaast ook enige subjectieve verwijtbaarheid kan worden aangetoond. Hiermee is – impliciet – een belangrijke safe harbor gegeven voor aanbieders waar deze objectieve elementen niet of amper aanwezig zijn: een technologieaanbieder wiens dienst of product maar in zeer beperkte mate inbreukmakend wordt gebruikt, en die bovendien geen (of een te verwaarlozen) financieel voordeel heeft van het inbreukmakend handelen, handelt in beginsel *niet* onrechtmatig, tenzij een actieve bijdrage of aanmoediging wordt aangetoond. Goede trouw mag hier naar mijn mening worden verondersteld. Deze safe harbor bevestigt de relevantie van de objectieve criteria: niet alleen speelt hun aanwezigheid een belangrijke (doch niet doorslaggevende) rol bij het oordeel over de onrechtmatigheid, andersom kan ook juist hun afwezigheid (in het voordeel van de aanbieder) duiden op niet-onrechtmatigheid. Bovendien maakt deze safe harbor duidelijk dat het substantial non-infringing uses criterium uit *Sony* nog steeds een belangrijk verweer kan zijn: dat een bepaald middel voor het overgrote deel legaal wordt gebruikt, is uiteraard een omstandigheid die meeweegt in het voordeel van de aanbieder.[58]

De tweede safe harbor die in de toets besloten ligt, heeft veel weg van de hosting-safe harbor in artikel 6:196c lid 4 (en de richtlijn Elektronische handel) respectievelijk paragraaf 512 van de DMCA. De aanbieder waarbij de objectieve elementen wél aanwezig zijn, ontsnapt (behoudens het geval van een actieve bijdrage of aanmoediging) aan aansprakelijkheid als hij een effectieve NTD-procedure heeft geïmplementeerd. Daaruit kan immers (doorgaans) worden afgeleid dat een aanbieder niet de intentie heeft om inbreuken te bevorderen.

Vooruitlopend op mogelijke kritiek: het probleem van subjectiviteit

Tegen de door mij geformuleerde toets zal men wellicht (kunnen) inbrengen dat, indien de '*subjectieve* wil' doorslaggevend is, dit onpraktisch is en kan leiden tot bewijsproblemen. Immers, hoe moet *daadwerkelijke* subjectieve intentie worden bewezen?[59] Onder juristen bestaat al jarenlang verschil van inzicht over de precieze betekenis van subjectiviteit bij de bepaling van aansprakelijkheid en over de vraag hoe het 'subjectieve' precies moet worden vastgesteld.[60] Heersende leer (die blijkt uit zowel rechtspraak als literatuur) lijkt te zijn dat hierbij geobjectiveerd mag worden, naar wat een normaal mens (de zogenaamde 'maatman') verweten kan worden. Gesproken wordt wel van de 'geobjectiveerde wil'. Alhoewel ik onderken dat het lastig kan zijn om een subjectieve intentie vast te stellen, meen ik dat de subjectieve dimensie in de door mij geformuleerde toets niet problematisch hoeft te zijn en dat de toets evenmin afbreuk doet aan de algemeen aanvaarde praktijk dat schuld 'objectief' wordt vastgesteld. Wel heb ik getracht grenzen te stellen aan die objectivering, om de (mogelijkheid van) aansprakelijkheid van technologie-aanbieders binnen de perken te houden.

Met de term 'subjectieve' verwijtbaarheid of intentie verwijs ik niet naar hetgeen zich in het hoofd van de internetaanbieder afspeelt of naar de persoonlijke capaciteiten van deze aanbieder. Een ingewikkelde zoektocht naar de motieven of opvattingen van de aanbieder kan achterwege blijven. Het gaat er, daarentegen, om wat *rechtens* heeft te gelden als de subjectieve wil van de aanbieder.[61] Daarom heb ik de subjectiviteit in de toets uitdrukkelijk gekoppeld aan het *zichtbare gedrag* van de technologieaanbieder: subjectieve verwijtbaarheid moet worden afgeleid uit (aanmoe-

57 Zie in dit verband ook de al eerder genoemde uitspraak van de rechtbank Amsterdam inzake *Brein/News-Service Europe* (Rb. Amsterdam 28 september 2011).

58 Zou de video- of dvd-recorder nu op de markt komen, dan zou de producent/ontwikkelaar ervan naar mijn mening niet onrechtmatig handelen. Van een actieve, inhoudelijke bijdrage is geen sprake: de bemoeienis van de dienstverlener (het verschaffen van de apparatuur) houdt op na het moment van verkoop en de producent kan niet weten wat er daarna mee gebeurt. Bovendien blijkt uit de praktijk dat video- en dvd-recorders voornamelijk voor legale doeleinden worden gebruikt, namelijk het opnemen van een programma voor later privé-gebruik (van illegaal, commercieel, gebruik zou pas sprake zijn indien de gemaakte kopie bijvoorbeeld later wordt verhandeld). De door mij geformuleerde safe harbor is dus van toepassing. Aansprakelijkheid van de aanbieder zou alleen op zijn plaats zijn als illegaal gebruik bij het moment van verkoop wordt aangemoedigd ('gebruik deze recorder om opnames te maken en deze vervolgens te verkopen').

59 K.J. Koelman, 'MGM vs. Grokster – AKA Auteursrecht vs. Techniek', *Computerrecht* 2005-39, p. 10.

60 Zo is Sieburgh van mening dat – bij het oordeel over 'subjectieve schuld' – de persoonlijke capaciteiten (kennis, inzicht, ervaring et cetera) van de dader betrokken moeten worden (C.H. Sieburgh, *Toerekening van een onrechtmatige daad* (diss. RUG), Deventer: Kluwer 2000). Anderen (waaronder Jansen) zijn van mening dat subjectieve verwijtbaarheid een onderzoek vereist naar de innerlijke gesteldheid (de psyche) van de dader en dat een feitelijk bij de dader bestaand bewustzijn of oogmerk moet worden aangetoond (K.J.O. Jansen, 'Het subjectieve element van de onrechtmatigheid', *NTBR* 2007-6, p. 222-228). Weer anderen (zoals van Dam) menen dat – door de mogelijkheid van objectivering van opzet en/of intentie, alsmede door de opkomst van verschillende risicoaansprakelijkheden – de mentale eigenschappen van de dader geen (noemenswaardige) rol meer spelen (C.C. Van Dam, *Zorgvuldigheidsnorm en aansprakelijkheid*, Deventer: Kluwer 1989).

61 K.O. Jansen, 'Het subjectieve element van de onrechtmatigheid', *NTBR* 2007-6, p. 222.

digende) uitlatingen en/of (inhoudelijke) handelingen van de technologieaanbieder. Dit gedrag mag bovendien objectief gekwalificeerd worden, in die zin dat van een objectief vergelijkingstype wordt uitgegaan.[62] Er zijn immers gevallen waarin de conclusie zich opdringt dat een technologieaanbieder – door zijn handelwijze – het bevorderen van inbreuken wel *moet hebben* beoogd of gewild. Daarvan zal doorgaans sprake zijn in geval van expliciete (of impliciete) aanmoediging of inhoudelijke bemoeienis van de aanbieder bij de door de gebruikers gepleegde inbreuken. In de specifieke context van peer-to-peer-programmatuur gaat de objectivering nog een stapje verder en mag zelfs de zogenaamde 'lineage' van een programma bij het oordeel over subjectieve intentie betrokken worden. In zo'n situatie staat het de aanbieder overigens vrij om een alternatieve (subjectieve) opvatting of verklaring voor het gedrag te geven, op basis waarvan toch anders geconcludeerd wordt. Ten slotte zij opgemerkt dat in de rechtspraak de tendens al steeds meer lijkt te verschuiven naar de (subjectieve) intentie. De rechter kijkt bijvoorbeeld steeds vaker naar de vraag met welk doel de dienst op internet wordt aangeboden. Subjectieve intentie wordt in de praktijk dus al belangrijk geacht, maar wordt als zodanig niet of onvoldoende wordt benoemd. Bovendien wordt die intentie thans vastgesteld aan de hand van verkeerde criteria (namelijk kennis, profijt en het percentage inbreukmakend gebruik).

Conclusie

Ondanks grote verschillen tussen het Amerikaanse recht, waar aansprakelijkheid moet berusten op een theorie van secondary liability, en het Nederlandse recht inzake de onrechtmatige daad, lijken de Nederlandse en Amerikaanse aanpak ten aanzien van de aansprakelijkheid voor het 'faciliteren van auteursrechtinbreuken' niet wezenlijk van elkaar te verschillen. Echter, in beide rechtsstelsels worstelen de rechters met de criteria om onrechtmatigheid vast te stellen. In de Verenigde Staten bestond – zelfs tussen rechters onderling – jarenlang verschil van mening over de juiste toepassing van de criteria voor vicarious- respectievelijk contributory liability. Alhoewel het Supreme Court in *Grokster* veel duidelijkheid verschafte door inducement naar voren te schuiven als doorslaggevend criterium voor aansprakelijkheid, liet het na te specificeren onder welke omstandigheden precies sprake is van de vereiste kwade intentie. In de Nederlandse rechtspraak concluderen de rechters doorgaans, aan de hand van een aantal terugkerende factoren, tot onrechtmatigheid, maar ligt de focus telkens op een ander criterium.

Uit de besproken rechtspraak komt sterk een zoektocht naar een werkbare methodologie om de onrechtmatigheid van het faciliteren van auteursrechtinbreuken te beoordelen, naar voren. In de huidige praktijk wordt te veel waarde gehecht aan geobjectiveerde factoren, die bij bijna elke internetdienstverlener wel aanwezig zijn en daarom minder relevant zijn. Bovendien ontbreekt een onrechtmatigheidstoets die de uitkomst van toekomstige zaken tegen 'faciliteerders' – zowel voor de aanbieders van technologie als auteursrechthebbenden – voorspelbaar maakt. Alhoewel een zekere onvoorspelbaarheid inherent is aan de zorgvuldigheidsnorm van artikel 6:162 BW, heb ik gepoogd om een dergelijke toets, onder de noemer 'subjectieve verwijtbaarheid', te formuleren. Van subjectieve verwijtbaarheid is sprake als een aanbieder de subjectieve intentie heeft om het inbreukmakend handelen te bevorderen, dan wel wanneer hij daaraan een substantiële bijdrage levert. Wil een internetdienstverlener vrijuit gaan, dan moet hij zich dus onthouden van elke actieve, inhoudelijke betrokkenheid bij de inbreuken en/of aanmoediging daarvan. Daarnaast verdient het aanbeveling om effectieve maatregelen (al dan niet in de vorm van een NTD-procedure) te treffen teneinde de schade van de rechthebbende(n) te voorkomen en/of beperken.

Of deze toets technologieaanbieders in alle gevallen vooraf zekerheid biedt, valt te bezien. Wel meen ik dat de hierboven geformuleerde toets in veel gevallen tot bevredigende resultaten zal leiden en een duidelijk(er) en eenduidig kader creëert voor onrechtmatigheid. Want daarop komt het, bij het vaststellen de onrechtmatigheid van het faciliteren van auteursrechtinbreuken, uiteindelijk neer: het vinden van het juiste evenwicht tussen het beschermen van auteursrechten op het internet en het niet onnodig verbieden van (nuttige) technologieën die belangrijke legale gebruiksmogelijkheden hebben.

62 G.H.A. Schut, 'Objectivering en subjectivering in het privaatrecht', in: P. Abas (red.), *Non sine causa* (Scholten-bundel), Zwolle: W.E.J. Tjeenk Willink 1979, p. 396-397.

63 Wellicht met uitzondering van *Zoekmp3*.