



FUTURE OF COPYRIGHT

OVER DE JURIDISCHE ASPECTEN VAN CREATIEVE UITINGEN

Technische maatregelen als middel tegen piraterij.

Wanneer het gaat om de distributie van digitale content, bevinden de entertainment industrie en consumenten zich eigenlijk al jaren in een soort patstelling. De consument wil overal en altijd toegang hebben tot digitale content tegen een redelijke prijs. De entertainment industrie wil dit graag aanbieden, maar is bang dat het zonder beperkingen ter beschikking stellen van al hun content zal leiden tot grootschalige piraterij en het hen onmogelijk maakt investeringen terug te verdienen. Het gevolg hiervan is dat consumenten en de entertainment industrie elkaar online niet goed genoeg weten te vinden, een situatie waar professionele piraten dankbaar gebruik van maken.

De oplossing ligt natuurlijk bovenal in het verbeteren van het digitale aanbod aan de consument. Het versnipperde en veelal beperkte aanbod dat er momenteel is zorgt ervoor dat consumenten illegale alternatieven opzoeken. Het bieden van een volwaardig alternatief voor het grote en eenvoudig toegankelijke illegale aanbod is absoluut noodzakelijk richting de toekomst. Maar de consument moet zich ook beseffen dat er niet zoiets is als gratis. Met name voor het maken van films en games zijn grote, risicovolle investeringen noodzakelijk. Deze moeten terugverdiend kunnen worden. Gebeurt dit niet, dan zullen er simpelweg geen films meer worden gemaakt. Eenzelfde redenering gaat op voor computerspellen en software. Daarom is effectieve bescherming van het auteursrecht richting de toekomst óók noodzakelijk.

Momenteel vindt de handhaving van het auteursrecht met name plaats via juridische weg en via Digital Rights Management (DRM). Bij juridische handhaving moet gedacht worden aan het vervolgen van professionele piraten (strafrechtelijk) en aan het vervolgen van consumenten (civielrechtelijk). Het vervolgen van individuele consumenten is overigens zeer omstreden en wordt met name door de filmindustrie gezien als een onwenselijke manier van handhaving. Handhaving via DRM betekent met name het reguleren van gebruik door middel van technologie (bijvoorbeeld kopieerbeveiliging). Maar ook deze methode is niet onomstreden. Naast het feit dat kopieerbeveiligingen over het algemeen snel doorbroken worden, beperkt het ook de goedwillende consumenten in het gebruik van hun legaal aangeschafte content.

Naast het voeren van rechtszaken (tegen professionele piraten) en handhaving via DRM moet er dus worden gezocht naar andere alternatieven. Het lijkt erop dat de ISPs richting de toekomst een sleutelrol zullen gaan vervullen bij het invullen van deze alternatieven omdat zij via hun netwerk het verkeer van en naar de illegale bronnen kunnen reguleren. Deze conclusie staat in een (nog geheim) rapport van het Engelse bedrijf Informa. In de studie is gekeken naar de verschillende manieren waarop ISPs zouden kunnen bijdragen aan het tegengaan en voorkomen van auteursrechtinbreuken.

Ook regulering door de ISP is omstreden. Hoewel het bij kan dragen aan een effectieve bestrijding van piraterij, bergt het ook risico's in zich voor de vrijheid van meningsuiting, privacy en de principes van netneutraliteit. Future of Copyright zal in de komende dagen verschillende technische maatregelen verkennen en de voors en tegens van regulering door de ISP op een rij zetten.

URL Blokkering

Wanneer een ISP van mening is dat via een bepaalde URL (domeinnaam) schadelijke of illegale content wordt aangeboden, dan heeft de ISP de mogelijkheid om deze URL te blokkeren. De meeste ISPs doen dit ook daadwerkelijk. Het gaat dan met name om domeinen waar illegale content zoals kinderporno wordt aangeboden. URL blokkering is een effectief mechanisme om directe downloads van download sites te blokkeren. Voor het tegenhouden van p2p-verkeer is het niet geschikt, omdat p2p-verkeer is opgebouwd uit talloze pakketjes die via verschillende IP-adressen worden binnengehaald. Wat wel een mogelijkheid is, is om p2p 'aggregators' zoals de Pirate Bay te blokkeren. Op deze manier zal het overgrote deel van de illegale downloaders afhaken.

Vanuit juridisch oogpunt is URL blokkering echter omstreden. URL blokkering staat namelijk op gespannen voet met de vrijheid van meningsuiting. Daarnaast kan een (naar achteraf blijkt) onterechte blokkade van een website een onrechtmatige daad jegens de betrokken site opleveren. De schade die voortvloeit uit de blokkade zou in theorie op de blokkerende ISP verhaald kunnen worden. Ook vanuit commercieel oogpunt kan het voor een ISP niet opportuun zijn om bepaalde sites te blokkeren. ISPs die actief download sites en Bittorrent trackers blokkeren zijn namelijk minder interessant voor consumenten die willen downloaden. Vanuit juridisch en commercieel oogpunt zijn ISPs daarom terecht terughoudend met het blokkeren van URLs en doen dit over het algemeen niet anders dan op last van de rechter. In Denemarken is onlangs op last van de rechter ISP Tele2 bijvoorbeeld gedwongen om toegang tot de Pirate Bay af te sluiten.

Protocol- en poortblokkering

Naast het blokkeren van een specifiek adres is het ook mogelijk om bepaalde transferprotocollen en de bijbehorende poorten te blokkeren. Moderne routers in het netwerk van de ISP maken het tegenwoordig mogelijk om verschillende vormen van IP-verkeer te herkennen. Zo kan een ISP bijvoorbeeld zien of er sprake is van Bittorrent, Skype, eDonkey, KaZaA of Napster verkeer. Vervolgens kan op basis van het geïdentificeerde type verkeer worden besloten om het te blokkeren. De meest eenvoudige manier is om de poort die het protocol gebruikt af te sluiten, maar moderne downloadprogramma's en protocollen hebben allerlei manieren om dit te omzeilen. Bijvoorbeeld door gebruik te maken van standaardpoorten (die niet afgesloten kunnen worden omdat dan essentiële diensten zoals mailen en surfen niet meer mogelijk zijn voor de klanten), of door telkens van poort te wisselen.

Hoewel de meeste ISPs terughoudend zijn in het blokkeren van protocollen en poorten, gebruiken diverse van hen de bovengenoemde methodes om hun netwerken of businessmodellen te beschermen. ISPs bijvoorbeeld die internetbellen niet toestaan zullen het VoIP protocol blokkeren. Maar over het algemeen zijn ISPs terughoudend met

het blokkeren van protocollen en poorten omdat het op gespannen voet staat met de principes van net-neutraliteit. Dit principe houdt in dat al het internetverkeer gelijkwaardig is en dus geen speciale behandeling mag krijgen. Daarnaast is het voor ISPs uit commerciële overwegingen vaak niet gunstig om poorten te blokkeren, veel consumenten zijn immers primair geïnteresseerd in downloaden. Echter, door de explosieve toename van het (Bittorrent) p2p-verkeer zien steeds meer providers zich genoodzaakt om toch grenzen te stellen, omdat de kosten voor het transport te groot worden en het de QoS van andere diensten zoals VoIP, streaming video, mail en websurfen aantast.

Bandwidth shaping en throttling

In het verlengde van protocol- en poortblokkering ligt 'bandwidth shaping' en 'throttling'. Hierbij grijpt de ISP in in het verkeer op zijn servers om de quality of service en veiligheid te garanderen. In tegenstelling tot protocol- of poortblokkering wordt niet de volledige verbinding afgesloten, maar wordt de snelheid van de verbinding tijdelijk teruggeschroefd en minder prioriteit gegeven aan het file sharing verkeer. Door het (tijdelijk) terugschroeven van p2p-verkeer kan genoeg bandbreedte worden gegarandeerd voor tijdkritieke toepassingen van andere gebruikers zoals streaming video, VoIP en webverkeer.

Wil een ISP aan bandwidth shaping en throttling doen, dan moet het verkeer wel herkend worden. Naast protocolherkenning wordt hiervoor ook zogenaamde Deep Packet Inspection (DPI) ingezet. DPI is een technologie waarmee niet alleen de header van een IP-pakket (waarin zaken als type verkeer, afzender en ontvanger staan) doorzocht kan worden, maar ook de data in het pakketje zelf (de payload). Op deze manier kan (nog) duidelijk(er) worden vastgesteld om wat voor verkeer het gaat. ISPs gebruiken DPI met name om het verkeer op hun netwerken beter te kunnen managen en om kwaadaardige IP-pakketten die voor aanvallen op het netwerk worden gebruikt te herkennen.

Het gebruik van Deep Packet Inspection is omstreden omdat ermee in de communicatie zelf gekeken kan worden. Een dergelijke mogelijkheid vormt natuurlijk een potentiële inbreuk op het recht op privacy van de abonnee. ISPs zullen daarom niet snel van deze technologie gebruik willen maken ten behoeve van derden zoals de overheid of de entertainment industrie. De vraag is wel in hoeverre er daadwerkelijk 'meegekeken' wordt door de ISP. Zo kan het kijken in de inhoud van één pakketje in principe al volstaan om te weten om welk protocol het gaat. Voor wat betreft content herkenning kan een klein aantal pakketjes al volstaan om vast te stellen of het wel of niet om een auteursrechtelijk beschermd werk gaat. Hoe het ook zij, het kijken in de payload van een IP-pakket is een in potentie meer inbreukmakende handeling dan het kijken naar de header en er zal dus zorgvuldig met de toepassing ervan moeten worden omgesprongen.

Filtering door content herkenning

Een laatste manier om ongewenste en illegale content te bestrijden is door het technisch mogelijk te maken om bestanden automatisch te herkennen. Wanneer bestanden automatisch herkend kunnen worden kan de doorgifte ervan geblokkeerd worden (filtering). Ook is het mogelijk om op p2p netwerken of Usenet te zoeken naar content die illegaal wordt verspreid (scanning). Om een bestand herkenbaar te maken kunnen

verschillende technieken worden gebruikt waaronder hash-matching, fingerprinting en watermarking.

Bij *hash matching* wordt er een rekenkundige formule toegepast op een bestand om zo tot een uniek getal te komen (een hash-waarde). Deze hash-waarde is uniek voor dit bestand en alle kopieën ervan. Door hash-waardes van bestanden te berekenen en deze tegen een database met bekende hash-waarden te houden kan bepaald worden of er match is. Een match betekent dat het gaat om een illegaal aangeboden werk. Een hashwaarde is uniek voor de bits waaruit het bestand wordt opgebouwd, niet de inhoud. Wanneer een bestand bijvoorbeeld wordt geconverteerd van .mpg naar .avi zal de hashwaarde niet langer overeenkomen.

Fingerprinting valt qua proces te vergelijken met hash-matching. Maar in plaats van de bits te herkennen wordt via fingerprinting de inhoud van een bestand herkend. De fingerprint wordt aan het originele bestand toegevoegd. Zelfs als het bestand wordt veranderd, blijft de fingerprint intact. Net als bij hash-matching wordt de fingerprint van een bestand vergeleken met bekende fingerprints in een database.

Bij watermarking wordt aan het bestand een (liefst) onzichtbaar watermerk toegevoegd. Dit watermerk is uniek geassocieerd met het bestand. Wanneer een bestand wordt gevonden kan aan de hand van het watermerk worden bepaald om welk bestand het gaat. Hiertoe wordt het watermerk gechecked tegen een database met watermerken.

Content herkenning heeft als grote voordeel dat schadelijke en illegale content wordt geblokkeerd of herkend, terwijl de legale transfer van bestanden niet wordt gehinderd. Maar het inrichten van een effectief systeem voor het herkennen van content is niet eenvoudig. Hoewel diverse providers content herkenning gebruiken voor het filteren van kinderpornografie, is er voor het filteren van auteursrechtelijk beschermde werken nog geen eenduidige oplossing. Dit heeft onder andere te maken met het feit dat het bij het verspreiden van auteursrechtelijk beschermde werken gaat het om meer bestanden en bestanden die groter zijn (waardoor ze vaak in delen worden getransporteerd). Dit maakt het herkennen van bestanden niet alleen moeilijker, maar bovenal is er vele malen meer rekenkracht voor nodig.

ISPs geven aan dat zij weliswaar content herkenning zouden kunnen inzetten, maar dat zij niet de kosten voor onder andere de benodigde rekenkracht niet (alleen) kunnen dragen. Daarnaast vormt het feit dat content herkenning voor auteursrechtelijk beschermde werken momenteel niet gestandaardiseerd is een probleem. Hierdoor moeten ISPs verschillende systemen inzetten en met verschillende rechthebbenden en hardware/software leveranciers in conclaaf. Een samenwerkingsverband tussen diverse rechthebbenden en leveranciers zou mogelijk een oplossing vormen, omdat de ISPs dan een centraal aanspreekpunt hebben en toegang tot een grotere database met controle bestanden

Conclusies

In de afgelopen dagen zijn verschillende technische maatregelen besproken die kunnen bijdragen aan het terugdringen van piraterij. Hoewel uiteraard geen van deze maatregelen 100% effectief is, is de verwachting wel dat de toepassing ervan wel tot een sterke reductie in de hoeveelheid illegaal uitgewisseld materiaal zal leiden.

Site blokkades

Het blokkeren van de toegang tot sites is het meest omstreden omdat dit ingaat tegen het recht op vrijheid van meningsuiting en informatiegaring. Professor Egbert Dommering noemt deze vorm van filtering zelfs censuur. Het blokkeren van sites is ook een redelijk 'grof' middel, ook bestanden die niet illegaal of auteursrechtelijk beschermd zijn worden op deze manier tegen gehouden.

Het blokkeren van sites zou dus enkel op last van de rechter moeten geschieden. Hierbij dient de rechter een afweging te maken tussen de belangen van de rechthebbenden en de beheerders van de site. Zaken als de schade aan de rechthebbenden, het belang van de vrijheid van meningsuiting en informatiegaring, de verhouding tussen legaal en illegaal aanbod en de manier waarop de site omgaat met Notice & Takedown verzoeken, kunnen aanknopingspunten voor de rechter zijn.

Poort- en protocolblokkering

Het blokkeren van poorten of protocollen is eveneens een grof middel om het illegaal uitwisselen van bestanden tegen te gaan, immers door de blokkade wordt ook de uitwisseling van legale bestanden getroffen. Dergelijke blokkades zijn niet goed voor innovatie op het gebied van distributie, treffen ook eerlijke gebruikers en remmen de ontwikkeling van nieuwe businessmodellen. Blokkades gericht tegen individuele gebruikers zijn wel mogelijk, maar dit zal dan een van de laatste stappen in een 'graduated' response procedure moeten zijn.

Bandwidth management

Het managen van bandbreedte is al een meer genuanceerde aanpak. Het terugschroeven van de snelheid van de verbinding zou bijvoorbeeld alleen die gebruikers kunnen treffen die boven een bepaalde downloadlimiet komen, of alleen die gebruikers die illegaal materiaal blijven up- en downloaden. Deze methode heeft ook als voordeel dat het nagenoeg niet ingrijpt in de vrijheid van meningsuiting, immers de informatie kan nog steeds worden overgebracht, zij het langzamer. Wel staat bandwidth management op gespannen voet met het beginsel van net-neutraliteit dat zegt dat al het internetverkeer gelijkwaardig is. Echter, gezien de exponentiële groei van het p2p-verkeer (tot momenteel zo'n 50% van de consumptie van bandbreedte wereldwijd) is het de vraag hoe lang dit principe überhaupt nog handhaafbaar is voor de ISPs.

Contentherkenning

Contentherkenning kan bijdragen aan het creëren van fijnmaziger systemen om piraterij tegen te gaan. Deze systemen zouden alleen die content kunnen blokkeren die daadwerkelijk illegaal verspreid wordt, zonder verder het overige p2p verkeer te storen. Nadeel van contentherkenning is dat de technologie nog volop in ontwikkeling is en de implementatie ervan relatief duur. Daarnaast speelt het feit dat naar de content gekeken moet worden hetgeen een mogelijke inbreuk op de privacy kan vormen.

Uit het bovenstaande blijkt dat het invoeren van technische maatregelen zeer zorgvuldig gebeuren. Omdat de toepassing van technische maatregelen op gespannen voet kan staan met de vrijheid van meningsuiting, de privacy van de gebruiker en de principes van net-neutraliteit, zijn transparantie, checks and balances en goede geschillenbeslechtingmechanismen noodzakelijk.

Naast de positie van de gebruiker speelt ook de positie van de ISP een rol. De ISP moet in principe niet op de stoel van de rechter terechtkomen. Toch lijkt het onvermijdelijk dat de ISPs keuzes zullen moeten gaan maken, hetzij op last van de rechter, hetzij ter bescherming van het eigen netwerk, hetzij in samenspraak met de rechthebbenden.



Except where otherwise noted, this work is licensed under <http://creativecommons.org/licenses/by-nc-sa/3.0/>