

De *broadcast flag* en fundamentele rechten:
verplichte kopieerbeveiliging in de Verenigde Staten

Ot van Daalen en Rik Lambers¹

1. Inleiding

Op 4 november 2003 heeft de *Federal Communication Commission* (FCC), de Amerikaanse regulator van de telecommunicatie- en mediasector, een maatregel aangenomen die de informatievrijheid, de innovatie en de vrije mededinging in vergaande mate beperkt: de *broadcast flag*.² De maatregel verplicht technologieproducenten om ontvangers van digitale televisiesignalen, zoals televisietoestellen en computerhardware, vanaf 1 juli 2005 uit te rusten met voorgeschreven technologie die een gesloten distributiekanaal kan garanderen. Dreiging van ongeautoriseerde distributie van digitale informatie via het internet zou dit rechtvaardigen.

Ook voor Europese ingezetenen heeft deze maatregel gevolgen. Hij zal de Amerikaanse afzetmarkt voor Europese technologieproducenten beperken, kan de Europese wetgever inspireren tot het aannemen van gelijksoortige wetgeving, en het gevaar bestaat dat hij een *de facto* standaard voor digitale televisie wordt.

Dit artikel behandelt de spanning tussen deze verplichte kopieerbeveiliging en fundamentele rechten, zoals de vrijheid van meningsuiting, en de vrije mededinging. Daarbij komt eerst de inhoud van deze regel aan bod, waarna wordt onderzocht in welk opzicht hij afwijkt van eerdere Amerikaanse en Europese regelgeving op het gebied van de informatiebeveiliging. Daarna komen de effecten voor gebruikersrechten, innovatie en mededinging aan de orde, waarbij tevens

¹ Ot van Daalen en Rik Lambers zijn werkzaam als onderzoeker bij het Instituut voor Informatierecht. Dit artikel is geschreven op persoonlijke titel. De auteurs bedanken Natali Helberger en Lodewijk Asscher voor hun commentaar.

² Federal Communications Commission 4 november 2003, 'Report and Order and Further Notice of Proposed Rulemaking', nr. MB 02-230, te vinden op: <http://www.eff.org/IP/DRM/HDTV/20031104_fcc_order.pdf>, hierna: 'FCC Report'. De regel is te vinden in 73 C.F.R. § 9000 e.v., en bouwt voort op een voorstel van een consortium waarin hardwareproducenten en contentindustrie deelnemen, zie Robert Perry, Michael Ripley en Andrew Setos, 'Final Report of the Co-Chairs of the Broadcast Flag Protection Discussion Subgroup to the Copy Protection Technical Working Group', 3 juni 2002, te vinden op: <<http://www.eff.org/IP/Video/HDTV/bpdg-report/>>, en een *Notice of Proposed Rulemaking* van de FCC, zie Federal Communications Commission 9 augustus 2002, 'Notice of Proposed Rulemaking In the Matter of Digital Broadcast Copy Protection', nr. MB 02-230, te vinden op: <<http://bpdg.blogs.eff.org/archives/nprm.pdf>>. In reactie hierop heeft de MPAA tezamen met een aantal hardwareproducenten op 6 december 2002 een voorstel voor mogelijke regelgeving ingediend, zie MPAA e.a., 'Joint Comments of the MPAA e.a.', 6 december 2002, te vinden op: <http://www.mpaa.org/Press/MPAA_Comments_02-230.pdf>. Dit voorstel is nadien gewijzigd.

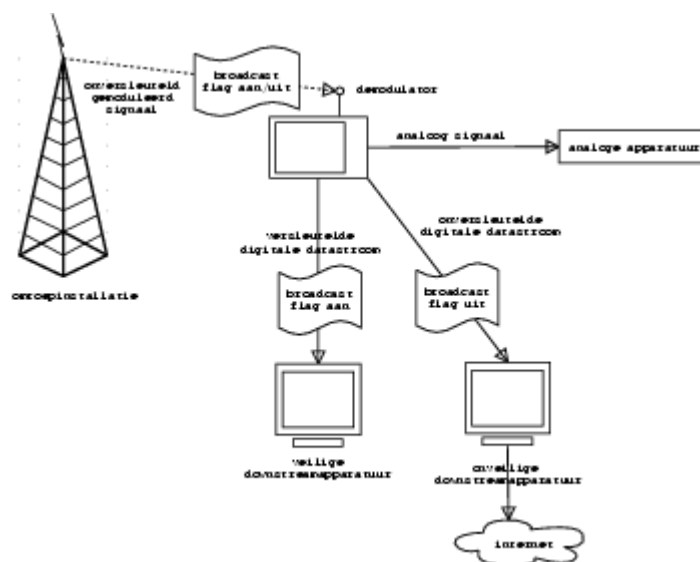
aandacht wordt besteed aan het Europese recht. Het artikel sluit af met enige kritische kanttekeningen.

2. De regels van de FCC

In Europa en de Verenigde Staten tracht de wetgever de overgang naar digitale televisie actief te bevorderen. Digitale signalen maken efficiënter gebruik van het frequentiespectrum dan analoge signalen, bieden ruimte voor het aanbieden van interactieve diensten, en kunnen zonder kwaliteitsverlies worden gereproduceerd.

Rechthebbenden vrezen echter voor ongeautoriseerde distributie via het internet als hun materiaal digitaal zal worden uitgezonden. Om de levensvatbaarheid van digitale televisie te waarborgen, tracht de FCC door de regulering van de *ontvangstmiddelen* van via de ether verspreide digitale televisie deze ongeautoriseerde redistributie te voorkomen.

Deze middelen mogen slechts digitale signalen redistribueren als een vlag die het signaal begeleidt, de *broadcast flag*, dit toestaat.³ Zo zouden rechthebbenden controle bewaren over de distributie van hun materiaal. Om een veilige behandeling van het digitale signaal te waarborgen dient ontvangstapparatuur te voldoen aan bepaalde ontwerpeisen, zodat een gemiddelde gebruiker deze niet kan aanpassen. Het is verboden om ontvangstmiddelen te verspreiden die niet voldoen aan de eisen van de FCC. De implementatie van dit systeem is geïllustreerd in figuur 1.



Figuur 1 De *broadcast flag* in beeld

³ Dit is de Redistribution control descriptor, ATSC Standard A/65B: Program and System Information Protocol for Terrestrial Broadcast and Cable, te vinden op: http://www.atsc.org/standards/a_65b.pdf, p. 78. Zij is reeds als standaard opgenomen door het lichaam dat standaarden vaststelt voor digitale televisie.

Een belangrijke vraag is hoe de FCC vaststelt welke ontvangstapparatuur mag worden verspreid. Zij heeft hierover in een *Further Notice of Proposed Rulemaking* belanghebbenden om nader commentaar gevraagd. Ondertussen heeft zij een voorlopige 'procedure op tegenspraak' aangenomen, binnen welk kader de FCC technologie op verzoek certificeert en belanghebbenden oppositie kunnen voeren. Bij certificering weegt de FCC onder meer de veiligheid, functionaliteit, interoperabiliteit en licentievoorwaarden van de onderzochte technologie.

De voorlopige procedure voorziet ook in de bevoegdheid van de FCC om het certificaat van technologie die niet meer veilig is - doordat deze gekraakt is - in te trekken. Dit biedt partijen een interessant wapen om ongewenste technologie van de markt te weren.

Voor technologieproducenten en gebruikers heeft deze maatregel vergaande gevolgen, welke in de volgende paragrafen aan de orde zullen komen. Om te illustreren hoezeer deze maatregel een *novum* is volgt hieronder een beschrijving van kopieerbeveiliging voorheen in de Verenigde Staten en Europa.

3. Kopieerbeveiliging voorheen

Een wettelijk regime om verplichte beveiligingstechnologie toe te passen, is slechts één keer eerder vertoond, in de Verenigde Staten. Dit liep uit op een mislukking. Afgezien daarvan hebben zowel de Europese als de Amerikaanse regelgever maatregelen genomen die slechts *vrijwillig* geïmplementeerde beveiligingstechnologie beschermen.

3.1 Kopieerbeveiliging in de Verenigde Staten

In 1992 heeft de Amerikaanse wetgever de Audio Home Recording Act (AHRA) aangenomen.⁴ Deze wet verplicht producenten van *digital audio recording devices* en *digital audio interface devices* om voorgeschreven kopieerbeveiliging, het zogenaamde *Serial Copy Management System* (SCMS) of een daarmee vergelijkbaar systeem, toe te passen.

De tekst is tegenwoordig een dode letter. Het Court of Appeals for the Ninth Circuit heeft op 15 juni 1999 in *RIAA v. Diamond Multimedia* uitgemaakt dat een mp3-speler niet onder deze bepalingen valt.⁵ De Amerikaanse muziekrechtshoudendeorganisatie *RIAA* stelde zich in deze zaak op het standpunt dat de producent van de Rio mp3-speler op grond van deze wet verplicht zou zijn om SCMS in haar apparatuur te verwerken. De rechtbank heeft echter overwogen dat een mp3-speler geen *digital audio recording device* is, omdat hij bestanden opslaat die afkomstig zijn van een harde schijf. Een harde schijf is niet te kwalificeren

⁴ Pub. L. No. 102-563 (1992). Deze wet is opgenomen in hoofdstuk 10 van de Amerikaanse auteurswet, 17 U.S.C. § 1001 e.v.

⁵ *Recording Industry Association of America v. Diamond Multimedia Systems Inc.*, 180 F.3d 1072 (9th Cir. 1999).

als een *digital audio recording*, terwijl de wet slechts ziet op apparatuur die muziek opslaat die hiervan afkomstig is. De wet bleek niet flexibel genoeg om het belangrijkste distributiemedium, de computer, te omvatten en is stil ten onder gegaan.

Inmiddels heeft de Amerikaanse wetgever nieuwe inzichten opgedaan over de wenselijkheid van verplichte kopieerbeveiliging. In 1998 heeft hij de Digital Millennium Copyright Act (DMCA) aangenomen, waarvan afdeling 1201 informatiebeveiligingsmaatregelen, zogenaamde technische voorzieningen, beschermt.⁶ Men mag op grond van dit artikel geen middelen verspreiden die zijn ontworpen om-, geen ander gebruik kennen dan-, of worden aangeprezen voor de omzeiling van technische voorzieningen. Maar afdeling 1201(c)(3), de zogenaamde *no mandate* bepaling, stelt uitdrukkelijk dat bovenstaande bescherming niet de plicht schept om informatietechnologie aan te passen aan een toegepaste beveiligingsmaatregel.

3.2 Kopieerbeveiliging in Europa

Ook de Europese regelgeving verplicht hardware- en softwarefabrikanten niet om hun producten aan een bepaalde beschermingsstandaard te laten voldoen.

Lid c van artikel 7 van de Softwarerichtlijn uit 1991 was de eerste Europese maatregel die kopieerbeveiligingsmechanismen beschermt.⁷ Dit artikel is gericht op middelen die *uitsluitend* bestemd zijn om een bescherming te omzeilen of te verwijderen. Artikel 4 van de Voorwaardelijke toegangsrichtlijn, de tweede maatregel hierover, verbiedt slechts middelen die zijn *ontworpen* of zijn *aangepast* om ongeautoriseerde toegang te verkrijgen tot een beschermde dienst.⁸

In de Auteursrechtverdragen, de meest recente Europese maatregel betreffende dit onderwerp, wordt zelfs *benadrukt* dat elektronica-producenten niet verplicht zijn tot het nemen van beschermingsmaatregelen.⁹ Overweging 48 bepaalt onder meer dat de bescherming van technische voorzieningen niet de verplichting inhoudt om 'inrichtingen, producten, onderdelen of diensten te ontwerpen die met technische voorzieningen overeenstemmen, voorzover dergelijke

⁶ Pub.L.No. 105-304 (1998). 17 U.S.C. § 1201.

⁷ Richtlijn 91/250/EEG, *PbEG* 1991, L 122/42. Deze bepaling is geïmplementeerd in artikel 32a van de Auteurswet.

⁸ Richtlijn 98/84/EG, *PbEG* 1998, L 320/54. Deze bepalingen zijn geïmplementeerd in artikel 326c van het Wetboek van Strafrecht.

⁹ Richtlijn 2001/29/EG, *PbEG* 2001, L 167/10. Artikel 6 is een implementatie van artikel 11 van het WIPO Auteursrechtverdrag (Wav), *Trb.* 1997, 318 (de Engelse en Franse tekst), en *Trb.* 1998, 247 (de Nederlandse tekst) en artikel 18 van het WIPO Verdrag inzake uitvoeringen en fonogrammen, *Trb.* 1997, 319 (de Engelse en Franse tekst), en *Trb.* 1998, 243 (de Nederlandse tekst).

inrichtingen, producten, onderdelen of diensten niet onder het verbod van artikel 6 vallen'.¹⁰

De FCC heeft gebroken met het Amerikaanse beleid, en haar maatregel wijkt ook af van Europese regelgeving op dit gebied. Het internet, dat vrije redistributie mogelijk maakt, zou volgens de FCC in de toekomst een bedreiging vormen van vrije, digitale televisie, en deze breuk met het verleden rechtvaardigen. Dit gaat zeer ver, en de wijze waarop de FCC deze bedreiging benadert, heeft de nodige kritiek gehad.

4. Kritiek

De kritiek richt zich ten eerste op de vraag of digitale televisie zich leent voor redistributie via het internet. Digitale televisiebestanden zijn vele malen groter dan muziekbestanden. Onder ideale omstandigheden, waarbij de gehele breedbandverbinding wordt benut, neemt het verzenden van een uur digitale televisie ongeveer veertig uur in beslag. Filesharing is daarmee onpraktisch, zo niet onmogelijk.¹¹ In dit licht zou de *broadcast flag* gezien moeten worden als een preventieve maatregel: 'We conclude that by taking preventive action today, we can forestall the development of a problem in the future similar to that currently being experienced by the music industry', aldus de FCC.¹² Daarmee neemt zij een krediet op de toekomst, en stelt innovatie en gebruikersrechten als onderpand.

De maatregel zou ten tweede niet geschikt zijn om het gestelde doel te verwezenlijken. De FCC maakt er geen geheim van wat het voornaamste doel van de *broadcast flag* is: '[...] the express goal of a redistribution control system for digital broadcast television [is] to prevent the *indiscriminate redistribution* of such content on the Internet'.¹³ Om dit te voorkomen creëert zij het digitale equivalent van een verkeersdrempel die is gericht op het voorkomen van 'casual copying'. Maar een dergelijke 'speed bump' kan 'indiscriminate distribution' niet tegengaan, zoals Princeton University hoogleraar Edward Felten terecht opmerkt.¹⁴ Ook al

¹⁰ Dit blijkt ook uit de toelichting bij de implementatiewet van deze richtlijn, waarin de minister overweegt dat de bedoeling van de regels niet is dat een technische voorziening de specificaties van apparatuur kan dicteren of de apparatuur tot wijziging van de functionaliteit kan dwingen, *Kamerstukken II* 28 482, nr. 3, p. 28. Zie ook p. 29 en p. 57. Artikel 6 bepaalt dat het aanbieden van omzeilingmiddelen en -diensten verboden is, voor zover deze worden geproduceerd-, geen ander doel hebben dan-, of in het bijzonder zijn ontworpen om de omzeiling mogelijk of gemakkelijker te maken van doeltreffende technische voorzieningen.

¹¹ Vergelijk de website van Public Knowledge, te vinden op:

<<http://www.publicknowledge.org/issues/broadcast-flag.html>>. Zie ook Electronic Frontier Foundation, 'Comments of Electronic Frontier Foundation', nr. MB 02-230, 6 december 2002, te vinden op: <<http://www.eff.org/IP/DRM/HDTV/20021206-eff-fcc-comments.pdf>>, p. 4-5, hierna 'EFF Report'.

¹² FCC Report, p. 5.

¹³ FCC Report, p. 6 (cursivering toegevoegd).

¹⁴ E. Felten 5 november 2003, vergelijk: <<http://www.freedom-to-tinker.com/archives/000469.html>>.

zou de gemiddelde gebruiker door deze drempel worden afgeremd – de enkeling die de *speed bump* neemt vormt reeds een lek.

De *broadcast flag* zou daarmee onderdeel zijn van een ontoereikend beveiligingsregime. De FCC onderkent dit, maar verwacht toch dat het door haar gekozen *threat model* voldoende effectief zal zijn.¹⁵

Het beveiligingsregime wordt tevens bedreigd door de zogenaamde *analog hole*. Terwijl de maatregel digitale televisiesignalen tracht te beschermen, laat het analoge signalen ongemoeid, opdat bestaande apparatuur kan blijven functioneren.¹⁶ Conversie van analoge naar digitale signalen blijft mogelijk, en de ongeautoriseerde redistributie van deze geconverteerde signalen dus ook.

Daarnaast is het de vraag of het beveiligingsregime te handhaven is. Zoals de FCC zelf toegeeft, zal ook na de implementatie van de *broadcast flag* verboden ontvangstapparatuur verkregen of gebouwd kunnen worden.¹⁷ De FCC ziet dit niet als een kritieke bedreiging: 'We do not believe, however, that individual acts of circumvention necessarily undermine the value and integrity of an entire content protection system'.¹⁸ Ook hier kan men zich afvragen of het middel wel geschikt is om het gestelde doel te verwezenlijken.

Tot slot heeft de maatregel belangrijke implicaties voor de vrijheid van meningsuiting, de innovatie en de mededing. Deze komen hieronder aan de orde.¹⁹

5. Implicaties voor fundamentele rechten

5.1 De informatievrijheid in de Verenigde Staten

De maatregel van de FCC tracht het gebruik van auteursrechtelijk beschermde werken te controleren door middel van de techniek. Het auteursrecht op een werk en de vrijheid van meningsuiting van een

¹⁵ FCC Report, p. 9-10. ('We are [...] mindful of the fact that it is difficult if not impossible to construct a content protection scheme that is impervious to attack or circumvention. We believe, however, that the benefits achieved by creation of a flag-based system *creating a 'speed bump' mechanism to prevent indiscriminate redistribution of broadcast content* and ensure the continued availability of high value content to broadcast outlets outweighs the potential vulnerability cited by commenters')(cursivering toegevoegd).

¹⁶ Vrijwel alle ontvangers van digitale televisie die op dit moment verkocht worden, bevatten een analoge uitgang, van waaruit het signaal weer kan worden gedigitaliseerd en verspreid. EFF Report, p. 11 en Center for Democracy and Technology, 'Implications of the Broadcast Flag: A Public Interest Primer', oktober 2003, te vinden op:

<<http://www.cdt.org/copyright/broadcastflag.pdf>>, p. 24, hierna 'CDT Report'. De FCC meende dat de *broadcast flag* daarom juist nu moest worden aangenomen, voordat het toenemend aantal onbeschermde ontvangers het analoge gat in een alles opslokkend zwart gat zou veranderen.

¹⁷ FCC Report, p. 9, EFF Report, p. 10 en CDT Report, p. 17.

¹⁸ FCC Report, p. 10.

¹⁹ De op privacy gestoelde vrijheid van 'intellectuele consumptie' wordt ook door de *broadcast flag* beperkt, maar komt hier verder niet aan bod. Vergelijk J. E. Cohen, 'DRM and Privacy', 18 *Berkeley. Tech. L.J.* 575 (2003).

gebruiker van dat werk kunnen conflicteren. De vrijheid van meningsuiting wordt, met name in de literatuur, in toenemende mate als afzonderlijke beperkingsgrond op het auteursrecht erkend.²⁰ Het Amerikaanse Supreme Court heeft een dergelijke beperking recentelijk echter nog als zeer uitzonderlijk bestempeld.²¹

De klassieke doctrine leert dat het auteursrecht een mogelijk conflict tussen het recht van de auteur en het recht op de vrijheid van meningsuiting internaliseert en oplost.²² Het auteursrecht zou reeds rekening houden met de belangen die de vrijheid van meningsuiting waarborgt, onder andere door toepassing van de *fair use*-doctrine.²³ *Fair use* staat het publiek toe een redelijk gebruik te maken van auteursrechtelijk beschermde werken. Een *fair use* kan bijvoorbeeld bestaan uit het maken van kopieën voor eigen gebruik, *time-shifting* (een programma opnemen en op een later tijdstip bekijken) of het downloaden van een programma voor educatieve doeleinden.

Voor de *fair use*-doctrine zijn twee verschillende legitimaties te onderscheiden.²⁴ De eerste is van utilistische, economische aard, ingegeven door de relatief hoge transactiekosten voor het betalen voor individueel gebruik en de onmogelijkheid het auteursrecht onder alle omstandigheden te handhaven. In een digitaal milieu zijn deze transactiekosten echter laag en maakt technologie de betaling voor minimaal gebruik en perfecte controle van dat gebruik mogelijk. Dit zou *fair use* in het digitale tijdperk kunnen reduceren tot een dode letter.

De tweede legitimatie beschouwt *fair use* inherent aan het auteursrecht, omdat het de vrije stroom van informatie die ten grondslag ligt aan de vrijheid van meningsuiting en het auteursrecht bevordert. Zij is niet slechts een imperfectie in de handhaving van het auteursrecht en heeft een bestaansrecht onafhankelijk van de technologische mogelijkheid daartoe.

Technische maatregelen die auteursrecht handhaven reflecteren niet noodzakelijkerwijs het besproken evenwicht tussen de vrijheid van meningsuiting en het auteursrecht. Zo lijkt de *broadcast flag* uit te gaan van de eerste, economische benadering. Zij dwingt absoluut af en het is

²⁰ Bijvoorbeeld Neil Weinstock Netanel, 'Locating copyright within the First Amendment skein', 54 *Stan. L. Rev.* 1 (2001) en Yochai Benkler, 'Free as the air to common use: First Amendment constraints on enclosure of the public domain', 74 *N.Y.U. L. Rev.* 354 (1999). Zie voor een Europees perspectief P.B. Hugenholtz, 'Auteursrecht contra informatievrijheid in Europa', in: A.W. Hins & A.J. Nieuwenhuis (red.), *Van ontvanger naar zender*, Amsterdam: Otto Cramwinckel 2003, p. 157-174.

²¹ *Eldred v. Ashcroft*, 537 U.S. 186 (2003).

²² Zie hierover Paul Goldstein, 'Copyright and the First Amendment', 70 *Colum. L. Rev.* 983 (1970) en Melville B. Nimmer, 'Does Copyright Abridge the First Amendment Guarantees of Free Speech and the Press?', 17 *U.C.L.A. L. Rev.* 1180 (1970).

²³ 17 U.S.C. § 107.

²⁴ Zie hierover Wendy Gordon, 'Fair Use as Market Failure: A Structural and Economic Analysis of the Betamax Case and Its Predecessors', 82 *Colum. L. Rev.* 1600 (1982).

onduidelijk of zij een redelijk gebruik van digitale televisie zal toelaten. Het 'oude' evenwicht tussen auteursrecht en de vrijheid van meningsuiting dreigt daarmee verstoord te worden ten nadele van de vrije informatiestroom.

De FCC stelt in ieder geval niet de intentie te hebben met de *broadcast flag* gebruik dat consistent is met het auteursrecht te hinderen.²⁵ Hoe aan deze intentie tegemoet te komen, wordt uitgesteld tot latere regulering, waartoe zij commentaar vraagt in haar *Further Notice of Proposed Rulemaking*. Als de *broadcast flag* al tegemoet zou komen aan de huidige vormen van *fair use*, dan blijft het probleem dat zij vormen die in de toekomst mogelijk legitiem worden beschouwd, dreigt uit te sluiten. Zij codeert dan als het ware het auteursrechtregime van vandaag voor morgen.

5.2 Innovatie en mededinging

Dat 'morgen' al 'vandaag' wordt vastgelegd door de *broadcast flag* is niet slechts bezwaarlijk voor *fair use* en aan de vrijheid van meningsuiting gerelateerde rechten voor gebruikers. Het draagt ook een gevaar in zich voor innovatie en vrije mededinging, en de transatlantische handel.

Innovatie is deels afhankelijk van de mogelijkheid van gebruikers te experimenteren met technologie, deze te bewerken en zo te komen tot nieuwe inzichten en toepassingen. De *broadcast flag* legt deze 'freedom to tinker' aan banden.²⁶

Daarnaast raakt technologische ontwikkeling onderhevig aan een beperkend kader, omdat toestemming is vereist om de marktplaats te betreden. Daarbij is van belang *wie* vaststelt dat technologie binnen dit kader valt, omdat deze als een poortwachter fungeert over de toetreding van nieuwe technologieproducenten, en daarbij eisen kan stellen die een anti-competitieve werking hebben.²⁷ Zoals gezegd heeft dit vooruitzicht de FCC doen besluiten in haar *Further Notice of Proposed Rulemaking* hierover nader commentaar te vragen.²⁸

Ook zal de maatregel de Amerikaanse afzetmarkt van Europese technologieproducenten beperken. In dit verband is interessant dat de Europese Commissie zich op het standpunt stelt dat het wettelijk verplichten van een standaard voor voorwaardelijke toegangssystemen in strijd is met artikel 49 van het EG Verdrag, dat de dienstenvrijheid beschermt.²⁹

²⁵ FCC Report, p. 6.

²⁶ Deze term is afkomstig van Edward Felten, die een weblog bijhoudt met een gelijkkluidende titel, zie <<http://www.freedom-to-tinker.org/>>.

²⁷ CDT Report, p. 17-18 + 28.

²⁸ FCC Report, p. 22.

²⁹ C. Llorens-Maluquer, 'European responses to bottlenecks in digital pay-tv: impacts on pluralism and competition policy', *Cardozo Arts & Ent. L.J.* 1998/2-3, p. 557-586.

Wellicht de belangrijkste vraag is in welke apparatuur de *broadcast flag* geïmplementeerd moet worden. Beperkt het zich tot speciaal voor de ontvangst van digitale televisie ontworpen elektronica, of strekt het zich uit over universele technologie, zoals de personal computer en het internet? De FCC geeft zelf het antwoord: "We further note that we intend our redistribution control regulations to apply to any device or piece of equipment whether it be consumer electronics, PC or IT device that contains a tuner capable of receiving over-the-air television broadcast signals".³⁰ Wanneer een computer een ontvangstkaart voor digitale televisie bevat en als *downstream* apparaat fungeert, dan moet de datastroom tussen die kaart en de overige applicaties, en uiteindelijk het internet, verlopen via een beveiligd kanaal. Hiermee schept de *broadcast flag* een precedent voor de mandatering van computertechnologie, en beïnvloedt ze de toekomst van het internet.

Een essentieel kenmerk van het ontwerp van het internet is de decentralisatie van controle. Deze is geplaatst aan het eind van het netwerk, bij de *end-user*, de gebruiker van de aangesloten computer. Het maakt de ontwikkeling van innovatieve toepassingen mogelijk zonder dat hiervoor toestemming nodig is van andere partijen. Ook de computer, ontworpen als open platform waarover de gebruiker controle uitoefent, staat deze innovatie toe.

De implementatie van de *broadcast flag* beperkt die openheid en ontnemt de gebruiker niet alleen de controle over beschermde inhoud, maar ook over een deel van zijn computer. Zo leidt de regulering van digitale televisie in naam van de bescherming van rechthebbenden tot een ingreep in de architectuur van computers en, in het verlengde, het internet.

In *Reno v. ACLU* verwierp het Amerikaanse Supreme Court nog de toepassing van het *broadcasting model* op het internet, en bood het de volledige First Amendment bescherming van het *print model*.³¹ Nu dreigt regulering naar televisiemaatstaven toch via de *ends* van het netwerk binnen te sluipen. Controle wordt verplaatst, open wordt gesloten.

Een voorbeeld van de innovatieve toepassingen die door deze regelgeving wordt bedreigd, is GNUradio.³² GNUradio is een zogenaamde *Software Defined Radio* (SDR). SDR's maken het mogelijk om met een antenne die op de computer is aangesloten signalen te ontvangen. Het verschil met eerdere generaties radio-ontvangers is dat de ontvangst voor een groot deel gebaseerd is op software, zodat deze radio's in hoge mate kunnen worden aangepast aan de wensen van de

³⁰ FCC Report, p. 18.

³¹ 528 U.S. 844 (1997). Voor een kritische analyse van de analoge toepassing van bestaande netwerk modellen op het internet, vergelijk: T. Wu, 'Application-Centered Internet Analysis', 85 *Virginia L. Rev.* 1165 (1999).

³² Zie de website: <<http://www.gnu.org/software/gnuradio/gnuradio.html>>.

gebruiker. Dit maakt een efficiënter gebruik van het spectrum mogelijk, maar ook de ontvangst van digitale televisie.

GNURadio wordt echter verspreid onder de GNU General Public License (GPL), een zogenaamde Free/Libre/Open Source Software licentie. De GPL geeft licentienemers de vrijheid om software die onder de GPL wordt uitgebracht te redistribueren en te wijzigen, mits deze wijzigingen onder dezelfde licentie worden uitgebracht. Dit maakt gedistribueerde software-ontwikkeling via het internet mogelijk, en heeft bijvoorbeeld geleid tot ontwikkeling van het GNU/Linux besturingssysteem.

GNURadio kan ook digitale televisiesignalen ontvangen, en is dus een ontvangstapparaat in de zin van de *broadcast flag*-maatregel. De vrijheid om deze software te wijzigen, die in de GPL is verankerd, staat echter op gespannen voet met de ontwerpeisen van de FCC, die onder meer bepalen dat apparatuur niet door de gebruiker kan worden gewijzigd. De regels van de FCC dreigen de ontwikkeling van een innovatieve toepassing als GNURadio tot stilstand te brengen.

6. Conclusie

Het auteursrecht op digitale televisie is een gerechtvaardigd belang, en verdient bescherming. Maar hoe zwaar dit belang ook weegt, rechtvaardigt het een mandatering van de *broadcast flag*?

Ons inziens niet. De FCC heeft een niet-effectieve, niet-proportionele maatregel aangenomen, die niet voldoet aan de eisen van subsidiariteit. De vraag rijst of de implementatie van een *broadcast flag* met Europees recht in strijd zou zijn, in het bijzonder met het recht op vrijheid van meningsuiting. De beantwoording hiervan hangt voor een deel af van in hoeverre de technologie die zal worden gecertificeerd, de informatievrijheid zal beperken. Maar ook zonder dat dit bekend is, is een voorlopige grondrechtelijke analyse informatief.

In het Autronic-arrest heeft het Europees Hof voor de Rechten van de Mens (EHRM) overwogen dat artikel 10 EVRM zich ook uitstrekt tot de ontvangstmiddelen.³³ De *broadcast flag* is een door de overheid gemandateerde beperking van de ontvangst- en redistributiemiddelen van digitale televisiesignalen, en dus een beperking in de zin van artikel 10 EVRM. Het tweede lid van dit artikel staat een dergelijke beperking toe 'indien die in een democratische samenleving noodzakelijk [is] in het belang van de bescherming [...] van de rechten van anderen', waaronder het auteursrecht.³⁴ Het is zeer de vraag of deze maatregel de noodzakelijkheidstoets zou doorstaan.

³³ EHRM 22 mei 1990, NJ 1991, 740, r.o. 47 (*Autronic AG v. Switzerland*).

³⁴ HR 20 oktober 1995, NJ 1996, 682, r.o. 3.11 (*Dior v. Evora*).

Zoals in de voorgaande paragrafen is aangegeven, is de regelgeving van de FCC niet direct noodzakelijk, omdat de huidige internetinfrastructuur onvoldoende bandbreedte biedt voor de onrechtmatige distributie van digitale televisie. Daarnaast is de regel niet geschikt om het gestelde doel te verwezenlijken: hij tracht *indiscriminate redistribution* op het internet te voorkomen, maar biedt slechts bescherming tegen *casual copying*. De vrijheid van meningsuiting, gebruikersrechten, innovatie en mededinging worden beperkt, om potentiële schade in de toekomst te voorkomen, waarvan niet eens zeker is of deze zich zal voordoen. De maatregel wijkt in sterke mate af van eerdere wetgeving, al was het maar in het negatieve uitstralingseffect dat hij heeft op informatietechnologie. Daarmee wordt een onwenselijk precedent geschepd.

Er bestaan daarnaast alternatieve maatregelen met minder schadelijke neveneffecten.³⁵ Ten eerste kunnen informatieproducenten de informatie aan de bron, dus bij het verlaten van de antenne, beveiligen door middel van encryptie. Dit beperkt ongeautoriseerde interceptie en redistributie, omdat slechts geautoriseerde hardwareproducenten de vereiste decryptietechnologie mogen licentiëren. Dit heeft tot gevolg dat de huidige televisietoestellen zonder deze decryptietechnologie zouden worden uitgesloten van ontvangst, en het zal tijd kosten om overeenstemming te bereiken over de gebruiken encryptiestandaard. Maar als de FCC deze overgang goed zou begeleiden is de maatregel meer proportioneel en beter geschikt om het gestelde doel te verwezenlijken.

Als alternatieve oplossing had zij ook maatregelen kunnen voorschrijven waarmee de herkomst van informatie kan worden achterhaald: het zogenaamde *fingerprinting* of *watermarking*. Dit voorkomt niet dat informatie zonder toestemming wordt geredistribueerd, maar vergemakkelijkt handhaving. Dergelijke technieken zijn nog niet voldoende veilig om vastberaden aanvallers te weerstaan, maar kennen wel minder verstrekkende gevolgen voor technologieproducenten en gebruikers.

Het is opmerkelijk dat hierover in Europa weinig discussie bestaat, want de *broadcast flag* heeft ook voor Europese ingezetenen gevolgen. Zoals in de inleiding is aangegeven kan deze maatregel de Europese wetgever inspireren, of zich ontwikkelen tot een *de facto* standaard. Daarnaast leidt de maatregel voor Europese informatietechnologieproducenten ertoe dat hun Amerikaanse afzetmarkt wordt beperkt, terwijl het Amerikaanse producenten

³⁵ Deze alternatieven worden ook door de FCC genoemd in hun rapport, zie FCC Report, p. 11-13.

toegestaan blijft om de verboden ontvangstapparatuur te produceren voor export.³⁶

Wellicht kan de Europese Commissie dit probleem naar voren brengen in de volgende onderhandelingsrondes over vrijhandel.

³⁶ Dit blijkt uit C.F.R. § 73.9009.