ABHANDLUNGEN ZUM
URHEBER- UND KOMMUNIKATIONSRECHT 55

Julia Fitzner

Von Digital-Rights-Management zu Content Identification

Neue Ansätze zum Schutz urheberrechtlich geschützter Multimediawerke im Internet

Eine technische, ökonomische und rechtliche Analyse

Nomos Stämpfli Verlag C. H. Beck

ABHANDLUNGEN ZUM
URHEBER- UND KOMMUNIKATIONSRECHT

des Max-Planck-Instituts für
Immaterialgüter- und Wettbewerbsrecht

Herausgegeben von
Josef Drexl
Reto M. Hilty
Gerhard Schricker
Joseph Straus

Band 55

Julia Fitzner

Von Digital-Rights-Management zu Content Identification

Neue Ansätze zum Schutz urheberrechtlich geschützter Multimediawerke im Internet

Eine technische, ökonomische und rechtliche Analyse

Nomos Stämpfli Verlag C. H. Beck

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: München, Ludwig-Maximilians-Univ., Diss., 2010

ISBN 978-3-8329-6652-2 (Nomos Verlag Baden-Baden)
ISBN 978-3-7272-1499-8 (Stämpfli Verlag AG Bern)

Die Schriftenreihe ist bis Band 51 beim Verlag C.H. Beck, München erschienen.

1. Auflage 2011

Für meinen Vater
Wolf E. Fitzner

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2010 von der juristischen Fakultät der Ludwig-Maximilians-Universität in München als Dissertation angenommen. Vor der Drucklegung wurden an der Arbeit zum Zwecke der Aktualisierung geringfügige Ergänzungen vorgenommen.

Ein herzliches Dankeschön gebührt zuvorderst meinem Doktorvater, Herrn Prof. Dr. Michael Lehmann, Dipl.-Kfm., der mir den Denkanstoß zu diesem Projekt gegeben hat und mich bei der Verwirklichung meines Forschungsvorhabens jederzeit mit Rat und Tat unterstützt hat. Besonders dankbar bin ich ihm dafür, dass er mich dazu angeleitet hat, meine während des LL.M.-Programms an der University of California at Berkeley sowie während der einjährigen Anwaltstätigkeit in New York gewonnenen Kenntnisse des anglo-amerikanischen Rechts für diese Arbeit fruchtbar zu machen. Weiterhin bedanke ich mich bei Herrn Prof. Dr. Dres. h.c. Joseph Straus für die zügige Erstellung des Zweitgutachtens sowie die Möglichkeit des Gedankenaustausches über Sinn und Unsinn von technischen Schutzmaßnahmen für digitale Multimediawerke.

Der Leitung des Max-Planck-Instituts für Immaterialgüter- und Wettbewerbsrecht, und hier an erster Stelle Herrn Prof. Dr. Reto M. Hilty, danke ich für die Aufnahme in das Stipendiatenprogramm. Vor allem die schier unbegrenzten Möglichkeiten der jurisdiktionsübergreifenden juristischen Recherche, die das Institut bietet, haben zum Gelingen der Arbeit wesentlich beigetragen. In diesem Zusammenhang bedanke ich mich auch bei Herrn Prof. Dr. Alexander Peukert und Frau Dr. Silke von Lewinski für ihre Betreuung während meiner Zeit als Stipendiatin am Institut.

Kaum gelungen wäre diese Arbeit jedoch ohne die unermüdliche Unterstützung meiner Familie, d.h. ohne Lutz' Toleranz, Geduld und unerschütterlichen Glauben an mich; ohne Rosemaries fortwährende Unterstützung, Motivation und psychologischen Beistand; ohne Mariannes und Kurts beständigen familiären Rückhalt. Ihnen allen spreche ich an dieser Stelle meinen tiefen Dank aus. Schließlich bedanke ich mich auch bei meiner Tochter Carla, die mir mit ihrem fröhlichen Naturell über so manche Durststrecke bei der Erstellung dieser Arbeit hinweggeholfen hat.

München, Mai 2011 Julia Fitzner

Inhaltsverzeichnis

Teil 1:
Einleitung

1. Kapitel: Einführung

„The answer to the machine is in the machine“[1] oder „the answer to the machine is not in the machine“:[2] sind technische, vor Umgehung rechtlich speziell geschützte Maßnahmen die adäquate Antwort auf die technischen Innovationen der Digitalisierung und die damit einhergehenden Gefahren für urheberrechtlich geschützte Musik- und Filmwerke („Multimediawerke“)? Die Beantwortung dieser Frage ist Gegenstand des ersten Schwerpunkts der vorliegenden Arbeit.

Ausgangspunkt ist die in den 90’er Jahren des letzten Jahrhunderts einsetzende Digitalisierung sowie deren Auswirkungen auf den Vertrieb von Multimediawerken. Die technische und rechtliche Reaktion hierauf lautete recht schnell, die mit der Digitalisierung und der zunehmenden globalen Vernetzung der Nutzer einhergehende Möglichkeit der unbeschränkten Vervielfältigung und Verbreitung von digitalen Inhalten weitestgehenden Restriktionen zu unterwerfen. In technischer Hinsicht geschah dies durch den Einsatz sogenannter „Digital-Rights-Management-Systeme“ („DRM-Systeme“), beispielsweise in Form von Kopierschutztechnologien im Zusammenhang mit dem Vertrieb von Musik-CDs, oder, etwas später, im Zusammenhang mit Downloads von Musiktiteln über das Internet. In rechtlicher Hinsicht dienten diesem Ziel Verbote betreffend die Umgehung von technischen Maßnahmen, die zum Schutz urheberrechtlich geschützter Werke eingesetzt werden („technische Schutzmaßnahmen“), sowie die Manipulation von Informationen, die den Rechtsinhabern[3] zur Wahrung und Durchsetzung ihrer Rechte dienen („Informationen zur Rechtewahrnehmung“). Solche Verbote wurden sowohl auf internationaler Ebene durch die WIPO-Internetverträge von 1996, als auch auf nationaler Ebene in den USA durch den Digital Millennium Copyright Act sowie in Europa bzw. in Deutschland durch die Multimediarichtlinie bzw. den ersten Korb der Urheberrechtsreform eingeführt.

1 *Clark*, in: *Hugenholtz* (Hrsg.), The Future of Copyright in a Digital Environment, 1996, S. 139 ff.
2 *Lehmann*, in: FS. *Pagenberg*, 2006, S. 413 ff.
3 Unter dem im Rahmen der vorliegenden Arbeit vorwiegend verwendeten Begriff des Rechtsinhabers sind alle Personen zu verstehen, die originäre oder derivative Inhaber der Rechte an urheberrechtlich geschützten Multimediawerken sind, vgl. *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 34 Rn. 14.

Damit richteten sich Technik und Recht jedoch gegen „des Pudels Kern", indem die hauptsächlichen Errungenschaften der Digitalisierung und globalen Vernetzung, nämlich die schier unbeschränkten Möglichkeiten der Vervielfältigung und Verbreitung digitaler Inhalte, neutralisiert werden sollten, um die tradierten Geschäftsmodelle der hiervon zunächst negativ betroffenen Industriezweige zu bewahren. Denn der wirtschaftliche Erfolg dieser Geschäftsmodelle hing davon ab, Gewinne hauptsächlich über den vollumfänglich kontrollierten Vertrieb von Multimediawerken über physische Datenträger zu erwirtschaften. Diese Kontrollierbarkeit des Vertriebs von Multimediawerken, die durch die neuen Vervielfältigungs- und Verbreitungsmöglichkeiten grundlegend in Frage gestellt worden war, sollte in der digitalen Ära durch technische und rechtliche Maßnahmen sichergestellt werden.

Die Auswirkungen dieser technischen und rechtlichen Maßnahmen, d.h. von DRM-Systemen und den sie flankierenden Rechtsetzungsakten auf internationaler und nationaler Ebene, auf das Urheberrecht wurden heiß diskutiert. Dabei wurden teilweise bereits Abgesänge auf das herkömmliche Urheberrecht angestimmt in der Erwartung, dass DRM-Systeme langfristig zu einer Aushöhlung oder gar zu einer Ersetzung des bisher geltenden Urheberrechts führen könnten.[4] Gegenstand der vorliegenden Arbeit ist es, vor diesem Hintergrund DRM-gestützte Geschäftsmodelle im Zusammenhang mit dem Vertrieb von Multimediawerken einer kritischen Analyse zu unterziehen. Ziel dieser Analyse ist, festzustellen, inwieweit diese Modelle und damit insbesondere auch der zu ihrer Unterstützung speziell gewährte rechtliche Schutz bisher erfolgreich gewesen sind. Nach fast 15 Jahren, die seit der Einigung auf die WIPO-Internetverträge und damit seit der ersten internationalen Reaktion auf die Auswirkungen der Digitalisierung auf das Urheberrecht vergangen sind, zieht diese Arbeit somit eine erste Bilanz in Bezug auf die wirtschaftlichen und rechtlichen Auswirkungen des Einsatzes von DRM-Systemen.

Der zweite Schwerpunkt dieser Arbeit widmet sich der zweiten Generation des Vertriebes und des Konsums von Multimediawerken über das Internet: der kommerziellen Nutzung von Multimediawerken im sogenannten „Web 2.0". Hier hat sich der Fokus des Vertriebs von Multimediawerken von den klassischen Intermediären, wie beispielsweise Tonträgerunternehmen oder Filmproduktionsfirmen, auf die Nutzer verlagert, die multimediale Inhalte auf entsprechenden Plattformen selbst erschaffen und anbieten.

Die urheberrechtliche Problematik des Web 2.0 besteht darin, dass die Nutzer hierüber nicht nur eigene Inhalte, sondern auch urheberrechtlich geschützte, fremde Multimediawerke ohne Erlaubnis der Rechtsinhaber der Öffentlichkeit zugänglich machen können und dies auch in großem Umfang praktizieren. In Bezug auf diese

4 Vgl. 5. Kapitel, Teil B.III.

Urheberrechtsverletzungen stellt sich auch die Frage nach der Haftung der Anbieter derjenigen Dienste, mit deren Hilfe die Nutzer urheberrechtswidrige Handlungen vornehmen, wie beispielsweise Videoplattformen und soziale Netzwerke („Web 2.0-Dienste"). Insoweit wurden zu einem recht frühen Zeitpunkt, nämlich im Zusammenhang mit der oben erwähnten Gesetzgebung zu technischen Schutzmaßnahmen und Informationen zur Rechtewahrnehmung, im US-amerikanischen Recht (17 U.S.C. § 512) und im deutsch-europäischen Recht (Art. 12 ff. der E-Commerce-Richtlinie, §§ 7 ff. TMG) spezielle Haftungsbeschränkungen für Internetanbieter („Internetserviceprovider" oder „ISPs") geschaffen. Diesen Haftungsbeschränkungen ist gemein, dass sie die Haftung von ISPs für Urheberrechtsverletzungen der Nutzer ihrer Dienste maßgeblich einschränken und darüber hinaus ISPs grundsätzlich von jeglichen Pflichten zur Überwachung ihrer Internetdienste freistellen.

Gerade im US-amerikanischen Recht wird von Seiten der Rechtsinhaber jedoch verstärkt die Frage gestellt, inwieweit diese Haftungsbeschränkungen oder zumindest die darüber hinaus bestehende weitgehende Freistellung von ISPs von jeglichen Überwachungs- und Kontrollpflichten in Bezug auf die im Rahmen ihrer Internetdienste begangenen Urheberrechtsverletzungen noch gerechtfertigt sind. Diese Problematik wird verschärft aufgrund neuer technischer Entwicklungen in Form von intelligenten Filtertechnologien, die eine inhaltliche Überprüfung und Identifizierung von urheberrechtlich geschützten Inhalten („content identification") zunehmend möglich machen („Content-Identification-Technologien").

Gegenstand des zweiten Schwerpunkts der vorliegenden Arbeit ist daher, die Auswirkungen dieser neuen technischen Möglichkeiten auf die Haftung und damit insbesondere auf die Anwendbarkeit der vorgenannten Haftungsbeschränkungen zugunsten von ISPs zu prüfen. Damit wird auch der zweite Schwerpunkt der speziellen Internetgesetzgebung der letzten 15 Jahre vor dem Hintergrund der tatsächlichen technischen Entwicklungen auf den Prüfstand gestellt. Es gilt herauszufinden, ob und inwieweit sich der Ansatz bewährt hat, Marktteilnehmer allein auf der Grundlage neuer technischer Gegebenheiten haftungsrechtlich zu privilegieren und welche Lehren hieraus zu ziehen sind.

2. Kapitel: Gang der Untersuchung

Wie soeben dargelegt wurde, wird im zweiten Teil der vorliegenden Arbeit die Effektivität des Einsatzes von DRM-Systemen beim Vertrieb von urheberrechtlich geschützten digitalen Multimediawerken analysiert. Zu diesem Zweck werden im dritten Kapitel zunächst die generellen Auswirkungen der Digitalisierung auf den Musik- und Filmmarkt dargestellt, einschließlich des Phänomens der Internetpira-

terie. Hieran schließt sich im vierten Kapitel eine Darstellung der technischen und ökonomischen Hintergründe und Grundlagen des Einsatzes von DRM-Systemen im Multimediabereich. Abgeschlossen wird dieser Abschnitt durch eine Schilderung der wesentlichen Rechtsakte, die zum Schutz technischer Schutzmaßnahmen bzw. Informationen zur Rechtswahrnehmung auf internationaler, US-amerikanischer, europäischer und deutscher Ebene erlassen wurden. Im Anschluss daran wird im fünften Kapitel dargelegt, dass der Einsatz von DRM-Systemen in einem der wichtigsten neuen Geschäftsfelder, die der Musikindustrie durch die Digitalisierung eröffnet wurden, dem Vertrieb von digitalen Tonaufnahmen in Form von Downloads über das Internet, gescheitert ist. Insoweit werden zunächst die Fakten zusammengestellt, die dieses Scheitern belegen, und im Anschluss die Gründe erläutert, die hierzu geführt haben. Als ein wesentlicher Faktor in diesem Zusammenhang wird zunächst die Beeinträchtigung wesentlicher Nutzerinteressen hinsichtlich Interoperabilität, Nachhaltigkeit der Nutzbarkeit sowie Daten- und Verbraucherschutz identifiziert. Des Weiteren spielt eine wesentliche Rolle die Schaffung eines vom eigentlichen Urheberrecht losgelösten „Paracopyright" durch die Einführung des speziellen gesetzlichen Schutzes in Bezug auf den Einsatz von DRM-Systemen. Hierin ist einer der wichtigsten Gründe für die fehlende Akzeptanz von DRM-Systemen durch die Nutzer zu sehen, an der der Einsatz von DRM-Systemen letztendlich gescheitert ist. Abschließend wird aufgezeigt, dass die Musikindustrie dieses Scheitern mittlerweile anerkannt hat und dabei ist, neue Strategien und Geschäftsfelder zu entwickeln, um auf die Herausforderungen der Digitalisierung zu reagieren.

Sodann befasst sich der dritte Teil der vorliegenden Arbeit mit den speziellen Herausforderungen, die nunmehr das sogenannte „Web 2.0" an den Schutz urheberrechtlich geschützter digitaler Multimediawerke stellt. Der Fokus liegt hierbei auf der Bekämpfung von Urheberrechtsverletzungen, die im Rahmen der typischen Internetdienste des Web 2.0 begangen werden, durch intelligente Filtertechnologien in Form von Content-Identification-Technologien. Zur Einführung in die Thematik werden im siebten Kapitel zunächst die Begriffe „Web 2.0" und „User Generated Content" sowie die Internetdienste, die in diesem Zusammenhang eine wichtige Rolle spielen, dargestellt. Daraufhin werden die Gefahren für urheberrechtliche Rechtspositionen kurz skizziert und ihnen die wesentlichen Errungenschaften und Chancen, die das Web 2.0 andererseits bietet, gegenübergestellt. Dabei wird vor allem auf das mit dem Web 2.0 einhergehende Vermarktungs- und Kommerzialisierungspotential für Multimediawerke eingegangen. Ein besonderes Augenmerk liegt insoweit auf der Kommerzialisierung von Multimediawerken im Rahmen von werbefinanzierten Geschäftsmodellen. Es folgt eine Darstellung der technischen Grundlagen von Content-Identification-Technologien. Weiterhin werden die wichtigsten Anbieter solcher Technologien sowie deren wesentliche Funk-

tionsweise kurz erläutert sowie die möglichen Einsatzfelder dieser neuen Technologien aufgezeigt.

Schließlich enthält das achte Kapitel eine rechtsvergleichende Darstellung der Auswirkungen von Content-Identification-Technologien auf die Haftung von Web 2.0-Diensten. Aufhänger dieser rechtlichen Analyse sind die derzeit vor allem in den USA zu beobachtenden Bestrebungen der Rechtsinhaber, ISPs mehr und mehr zu einer proaktiven Überwachung ihrer Internetdienste auf Urheberrechtsverletzungen zu drängen. Prominentestes Beispiel hierfür ist die im Jahr 2007 von Viacom gegen Google und deren Tochter YouTube erhobene, mittlerweile erstinstanzlich entschiedene Klage und der darin liegende Versuch, ISPs im großen Umfang für die Urheberrechtsverletzungen ihrer Nutzer in die Haftung zu nehmen. In diesem Zusammenhang spielt wiederum der Einsatz von Content-Identification-Technologien eine wesentliche Rolle, wie sich beispielsweise an den „User Generated Content Principles" zeigt. Vor diesem Hintergrund ist Ziel der rechtsvergleichenden Analyse, festzustellen, inwieweit ISPs zum Einsatz von Content-Identification-Technologien nach der derzeitigen US-amerikanischen und deutsch-europäischen Rechtslage gezwungen werden können bzw. deren Einsatz sich auf ihre Haftung positiv oder negativ auswirkt. Eine wesentliche Rolle spielen in diesem Zusammenhang die speziellen Haftungsbeschränkungen für ISPs in Form von 17 U.S.C. § 512, Art. 12-15 der E-Commerce-Richtlinie und §§ 7-10 TMG. Abgeschlossen wird die Arbeit im vierten Teil durch eine Zusammenfassung und kritische Betrachtung der gefundenen Ergebnisse.

Teil 2:
Das Scheitern von Digital-Rights-Management-Systemen beim Vertrieb von Musikdownloads über das Internet

3. Kapitel: Der Markt für Multimediawerke im Zeitalter der Digitalisierung

A. Auswirkungen der Digitalisierung auf die Strukturen der Multimediaindustrie

Der Markt für Multimediawerke befindet sich seit Anbruch der digitalen Ära in einer Situation des Umbruchs, die bis heute noch nicht vollständig abgeschlossen ist. Durch die Digitalisierung wurden die Regeln, die bisher für die Kommerzialisierung urheberrechtlich geschützter Multimediawerke galten, in ihren Grundfesten erschüttert. Im Zentrum des sogenannten „digitalen Dilemmas" steht die Frage, ob und in welchem Umfang mit dem Vertrieb von Multimediawerken noch Geld verdient werden kann, wenn die Nutzer schnell, kostengünstig und ohne jeglichen Qualitätsverlust digitale Vervielfältigungsstücke von Multimediawerken selbst herstellen und im Anschluss daran über das Internet weltweit an andere Nutzer weiterverbreiten können.[5]

Multimediawerke sind in Bezug auf die Art und Weise, wie sie konsumiert und verbreitet werden können, wesentlich von den jeweiligen technologischen Gegebenheiten abhängig.[6] Denn zur Herstellung von Multimediawerken sind technische Hilfsmittel unabdingbar und gleichzeitig Voraussetzung dafür, dass das Multimediawerk einer breiten Öffentlichkeit zugänglich gemacht werden kann. Daher werden die Geschäftsmodelle zur Produktion, Verbreitung und Vermarktung von Multimediawerken sowie die an diesen Prozessen beteiligten Unternehmen besonders stark von neuen technologischen Entwicklungen beeinflusst. Nachdem die Industriezweige, die von der Kommerzialisierung von Multimediawerken leben („Multimediaindustrie"), in den letzten hundert Jahren bereits wiederholt auf die Einführung neuer Technologien zum Konsum und zur Verbreitung von Multimedia-

5 *Ünlü*, Content Protection, 2005, S. 44.
6 *Krasilovsky/Shemel*, Music Business, 2007, S. 414 ff.

werken reagieren mussten, gilt es nunmehr die Herausforderungen des digitalen Zeitalters zu meistern.[7]

I. Musikindustrie

> „I don't even know why I would want to be on a label in a few years, because I don't think it's going to work by labels and by distribution systems in the same way ... . The absolute transformation of everything that we ever thought about music will take place within 10 years, and nothing is going to be able to stop it. ... Music itself is going to become like running water or electricity ... . It's terribly exciting. But on the other hand it doesn't matter if you think it's exciting or not; it's what's going to happen."[8]

Im Rahmen der Diskussionen um die Auswirkungen der Digitalisierung auf die Multimediaindustrie steht die Musikindustrie seit jeher im Fokus, da sie von den mit der neuen Ära einhergehenden technischen und vor allem ökonomischen Folgen bislang am stärksten betroffen ist.[9] Der weltweite Gesamtumsatz der Branche mit Tonträgern geht seit Ende des letzten Jahrtausends kontinuierlich zurück. Betrug der Gesamtumsatz im Rekordjahr 1999 über US$ 40 Milliarden, so lag er im Jahr 2009 nur noch bei knapp US$ 25 Milliarden, was einem Umsatzrückgang von 37,5 Prozent entspricht.[10]

1. Strukturen der US-amerikanischen Musikindustrie bis zur Einführung der CD

In den USA verzeichnete die Musikindustrie seit Mitte der 50'er bis Anfang der 80'er Jahre des vorigen Jahrhunderts ein beständiges Wachstum von jährlich durchschnittlich 20 Prozent,[11] so dass der Gesamtumsatz der Branche im Jahr 1978

7 Im Musikbereich die Einführung des sogenannten „player piano", der Langspielplatte, der Musikkassette und der Compact Disc; im Filmbereich die Einführung von Rundfunk, Fernsehen und Video. Allerdings resultierten all diese technischen Neuerungen im Ergebnis in einer wirtschaftlichen Stärkung der Multimediaindustrie. Beispielsweise eröffnete die Einführung von Videokassette und –recorder der Filmindustrie sehr lukrative neue Einnahmequellen. Mit den technischen Nachfolgern von Videokassette und –recorder, d.h. mit DVD– und BluRay-Playern und –speichermedien generiert die Filmindustrie gegenwärtig den Löwenanteil ihrer Umsätze; s.a. *Krasilovsky/Shemel*, Music Business, 2007, S. 5, 414 ff.

8 *David Bowie*, zitiert bei *Pareles*, David Bowie, 21st-Century Entrepreneur, The New York Times, 9.6.2002, http://www.nytimes.com/2002/06/09/arts/music/09PARE.html (zuletzt abgerufen am 01.07.2010).

9 Vgl. hierzu etwa den Beitrag „Wirtschaftlichkeit in der Musikindustrie" von *Jacob*, in: *Clement/Schusser/Papies* (Hrsg.), Ökonomie Musikindustrie, 2008, S. 76 ff.

10 *Bundesverband der Musikindustrie*, Musikindustrie in Zahlen 2009, S. 58.

11 *Krasilovsky/Shemel*, Music Business, 2007, S. 5.

erstmalig mehr als US$ 4 Milliarden betrug. Der Tonträger war gleichsam „das Sinnbild der Musikindustrie", dessen Produktion, Vermarktung und Vertrieb an die Nutzer im Mittelpunkt stand.[12] Vor allem aus Gründen der Klangoptimierung wurde das Format der Tonträger in regelmäßigen Abständen und in Abhängigkeit von den zur Verfügung stehenden Technologien überarbeitet.

So kam es im Jahr 1984 zur Einführung der Compact Disc („CD"), dem ersten digitalen Massenprodukt der Konsumelektronik, die den Anbruch der digitalen Ära für die Musikindustrie markierte. Die CD löste einen massiven Anstieg der Umsätze aus:[13] Im Jahr 1988 wurden mit dem Verkauf von Langspielplatten („LPs"), Musikkassetten („MCs") und CDs insgesamt Einnahmen in Höhe von US$ 6,25 Milliarden erzielt, zehn Jahre später – unter der zusätzlichen Berücksichtigung von Einnahmen im Zusammenhang mit Musikvideoprodukten – bereits US$ 13,7 Milliarden.[14] Aufgrund des digitalen Formats der auf der CD als Dateien gespeicherten Tonaufnahmen konnten diese nicht nur auf einem CD-Player, sondern mit Hilfe eines CD-Lesegeräts auch auf einem Computer abgespielt und Kopien dieser Dateien mit Hilfe des Computers erstellt und auf dessen Festplatte abgespeichert werden. Anfangs waren solche CD-Lesegeräte noch teuer und es bestand noch nicht die Möglichkeit, Kopien dieser Dateien mit Hilfe von Computernetzwerken oder über das Internet im großen Stil an Dritte weiterzuverbreiten. Daher führte die Einführung der CD zunächst zu einem Boom in der Musikindustrie, da viele Nutzer ihre Musiksammlungen weitgehend durch das neue Format ersetzten.[15] Dies änderte sich jedoch abrupt Mitte der 90'er Jahre des letzten Jahrhunderts. Denn die technischen Fortschritte im Bereich der Komprimierungstechnologien führten zu einem Preisverfall für Kopiersoftware und CD-Lese– und –Brenngeräte.[16] Zudem führte die fortschreitende Verbreitung des Internets sowie die Ersetzung des für Musikdateien ursprünglich genutzten WAV-Formats durch das auch heute noch überwiegend genutzte MP3-Format zu einer drastischen Vereinfachung der Vervielfältigung und Übermittlung von Musikdateien über digitale Netzwerke.[17] All

12 *Reinke*, Wertschöpfungsmöglichkeiten Musikindustrie, 2009, S. 17.
13 *Bernstein/Sekine/Weissman*, Global Music Industry, 2007, S. 15.
14 *Krasilovsky/Shemel*, Music Business, 2007, S. 5-6.
15 *Reinke*, Wertschöpfungsmöglichkeiten Musikindustrie, 2009, S. 17.
16 *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 18.
17 Im WAV-Format besaß ein durchschnittliches dreiminütiges Musikstück noch eine Dateigröße von ca. 50 Megabytes, was unter der Nutzung einer ISDN-Internetverbindung einer Dauer von etwa 1 1/2 Stunden entsprach, um die Datei über das Internet an einen anderen Computer zu übermitteln. Da es zu diesem Zeitpunkt noch kaum Flatrates gab, bedeutete eine solche langwierige Übertragung gleichzeitig hohe Kosten für die damit verbundene Nutzung der Telefonverbindung und des Internetanschlusses. An die Übertragung schloss sich das Problem der Speicherung der Datei aufgrund der begrenzten Kapazität der Festplatte des empfangenden Computers. Hingegen wird im seit etwa 1998 überwiegend genutzten

diese Umstände resultierten in erheblichen Umsatzrückgängen der Musikindustrie.[18]

Zuvor, d.h. in der Zeit vor Anbruch der Ära der Digitalisierung, zeichnete sich die Musikindustrie durch eine jahrzehntelange strukturelle Stabilität aus.[19] Ihr wirtschaftlicher Erfolg basierte vor allem auf der Tätigkeit der Tonträgerunternehmen im Zusammenhang mit dem Vertrieb von Tonaufnahmen auf physischen Datenträgern sowie auf den Rechten, die das Urheberrecht denjenigen garantierte, die an der Herstellung, Verbreitung und Vermarktung dieser Tonaufnahmen beteiligt waren.[20] Die klassische Wertschöpfungskette bestand aus fünf Faktoren (Beschaffung der Inputfaktoren, Musikproduktion, Rechtehandel, Tonträgerproduktion und Absatz),[21] die weitgehend von den Tonträgerunternehmen wahrgenommen wurden. Dabei stellte sich die Aufgabe, Tonaufnahmen zu produzieren und zu vertreiben, insgesamt als ein risikoreiches und kostspieliges Unterfangen dar. Denn der Erfolg einer künstlerischen Unternehmung konnte niemals mit Sicherheit vorhergesagt werden. Weiterhin überstiegen die für die Herstellung, Vermarktung und Verbreitung einer Tonaufnahme zunächst aufzubringenden finanziellen Mittel regelmäßig das Budget eines durchschnittlichen Künstlers am Anfang seiner Karriere, so dass diese Kosten immer vom Tonträgerunternehmen vorgestreckt werden mussten.[22]

Im Gegenzug für die Übernahme dieses künstlerischen und finanziellen Risikos ließen sich die Tonträgerunternehmen von den von ihnen unter Vertrag genommenen Künstlern Rechte in Bezug den Tonaufnahmen einräumen, insbesondere den Anspruch auf den Löwenanteil an den durch den Vertrieb der Tonaufnahme zu erzielenden Einnahmen. Um das wirtschaftliche Risiko möglichst zu minimieren, übernahmen die Tonträgerunternehmen möglichst viele neue Künstler in ihr Portfolio, um die unvermeidbaren wirtschaftlichen „Flops“ mit möglichst vielen

MP3-Format eine durchschnittliche Musikdatei auf eine Größe von etwa 1,25 Megabytes komprimiert, so dass sie ohne großen Aufwand an Zeit und Speicherkapazität schnell und einfach über das Internet übertragen werden kann. MP3 steht als Abkürzung für „MPEG-1 Audio Layer 3“, ein Format, das ab 1982 am Fraunhofer-Institut für Integrierte Schaltungen (IIS) in Erlangen sowie an der Friedrich-Alexander-Universität Erlangen-Nürnberg in Zusammenarbeit mit AT&T Bell Labs und dem französischen Elektronikunternehmen Thomson entwickelt wurde. Vgl. hierzu beispielsweise *Haring*, MP3, 2002, S. 36 ff; s.a. *Krasilovsky/Shemel*, Music Business, 2007, S. 422.

18 *Reinke*, Wertschöpfungsmöglichkeiten Musikindustrie, 2009, S. 17.

19 *Krasilovsky/Shemel*, Music Business, 2007, S. 426.

20 *Schultz*, 43 U. Rich. L. Rev. 685, 690 (2009).

21 Vgl. *van Dyk*, in: *Clement/Schusser/Papies* (Hrsg.), Ökonomie Musikindustrie, 2008, S. 198; *Reinke*, Wertschöpfungsmöglichkeiten Musikindustrie, 2009, S. 19.

22 *Schultz*, 43 U. Rich. L. Rev. 685, 690 (2009); *Einhorn,* Gorillas in Our Midst, 2007, S. 2; dementsprechend vergleicht *Jakob* die Musikindustire mit einer Venture Capital Firma, die in eine Vielzahl von “Start-Ups” investiert und hofft, dass einer von zehn Künstler ein “IPO” in Form eines Superstars wird, *Jacob*, in: *Clement/Schusser/Papies* (Hrsg.), Ökonomie Musikindustrie, 2008, S. 77.

erfolgreichen Neuerscheinungen zu kompensieren.[23] Die Durchsetzbarkeit und mithin die Werthaltigkeit der den Tonträgerunternehmen in Bezug auf die Tonträger zustehenden bzw. von den Künstlern eingeräumten Rechtspositionen, von denen der wirtschaftliche Erfolg dieser Unternehmen maßgeblich abhing, wurde durch das Urheberrecht garantiert. Das Urheberrecht leistete somit einen maßgeblichen Beitrag dazu, dass die Tonträgerunternehmen das mit dem Aufbau neuer Künstler verbundene unternehmerische Risiko übernehmen konnten.[24]

2. Strukturelle Veränderungen seit Anbruch des digitalen Zeitalters

Tonträgerunternehmen spielen im Musikmarkt auch zum gegenwärtigen Zeitpunkt immer noch eine tragende Rolle. Die vier größten Unternehmen der Branche („Major Labels") sind Sony Music Entertainment („Sony"), Universal Music Group („Universal"), EMI Music („EMI") und Warner Music Group („Warner"), zu denen etwa 40 verschiedene Musiklabel gehören, unter denen die unter Vertrag genommenen Künstler jeweils vermarktet werden. Diese Major Labels erwirtschaften ca. 75 bis 80 Prozent der insgesamt im US-amerikanischen Markt mit dem Vertrieb von Tonaufnahmen erzielten Umsätze.[25] Allerdings sehen sich gerade die Tonträgerunternehmen aufgrund der technischen Neuerungen und der mit der Verbreitung des Internets einhergehenden weltweiten Vernetzung der Nutzer gleichzeitig vor mehrere Herausforderungen gestellt, von denen bereits jede einzelne dazu ausreichen würde, tiefgreifende Veränderungen in der Branche auszulösen: die Revolutionierung der technischen Grundlagen von Produktion und Vertrieb, die Verlagerung und Dezentralisierung des Marketings sowie das Schrumpfen des Marktes für physische Datenträger.

a. Revolutionierung der technischen Parameter betreffend die Produktion und den Vertrieb von Tonaufnahmen

Bisher musste ein Tonträgerunternehmen, um einen neuen Künstler oder eine neue Band herauszubringen („Neuerscheinung"), ca. US$200.000 bis US$300.000 zur Aufnahme des sogenannten „master recording" und der Produktion der entsprechenden physischen Datenträger, auf denen das *master recording* vertrieben wurde, vorlegen, im Falle bereits etablierter Künstler oft auch ein Vielfaches mehr.[26] Diese

23 *Schultz*, 43 U. Rich. L. Rev. 685, 690 (2009).
24 *Schultz* s.o.
25 *Einhorn*, Gorillas in Our Midst, 2007, S. 2.
26 *Perritt*, 16 Mich. St. J. Int'l Law 113, 1120 (2007).

Kosten zur Herstellung von Tonaufnahme und -trägern wurden jedoch zum einen durch die Verfügbarkeit digitaler Aufnahme- und Bearbeitungstechnologien und -software wesentlich verringert.[27] Zum anderen schrumpfen insbesondere die Kosten für die Produktion und den Vertrieb von Tonträgern aufgrund der zunehmenden Verbreitung des Internets, wodurch die Notwendigkeit einer analogen Vertriebsstruktur aufgrund der Möglichkeit des Vertriebs von Musiktiteln und –alben in rein digitaler Form mehr und mehr entfällt. Demgegenüber erhöht sich das Verbreitungspotential von digitalen Inhalten über das Internet zunehmend aufgrund der ständig steigenden Reichweite dieses Mediums.[28] Dadurch entfällt jedoch ein großer Teil der Kosten für die Herstellung, die Lagerung, den Transport und die Lieferung von physischen Datenträgern ersatzlos, wie sie bisher beim Vertrieb von Langspielplatten, Musikkassetten und CDs über Einzelhändler angefallen sind. Es ist daher nicht mehr ausgeschlossen, dass ein Künstler den Aufwand der Herstellung einer Tonaufnahme alleine schultert,[29] indem er mit Hilfe eines Computers und entsprechender Software die Tonaufnahme selbst digital im MP3-Format aufnimmt. Im Anschluss daran kann er diese Aufnahme selbst über das Internet vertreiben, beispielsweise durch ihre Einstellung auf einer Musikplattform wie MySpace Music, durch die Versendung der MP3-Datei per Email an potentielle Interessenten oder durch Nutzung eines Internetdienstes wie beispielsweise CDBaby, der kostengünstig die Produktion von Datenträgern anbietet. Im Zeitalter der Digitalisierung und der zunehmenden Verbreitung von Breitband-Internetanschlüssen können Tonaufnahmen somit unmittelbar vom Musiker an den Rezipienten vertrieben werden, ohne dass hierzu ein Intermediär in Form eines Tonträgerunternehmens notwendigerweise zwischengeschaltet werden muss.[30]

b. Verlagerung und Dezentralisierung der Vermarktungswege

Darüber hinaus ergeben sich aufgrund der vielfältigen Kommunikationsmöglichkeiten, die das Internet beispielsweise in Form sozialer Netzwerke bietet,[31] neue Vermarktungswege, die von den traditionellen, weitgehend von den Major Labels dominierten Kanälen unabhängig sind und diese mehr und mehr ersetzen.

Bisher investierten die Tonträgerunternehmen, sobald das *master recording* und die Tonträger produziert waren, zusätzliche hohe Beträge in die Vermarktung der

27 *Van Dyk*, in: *Clement/Schusser/Papies* (Hrsg.), Ökonomie Musikindustrie, 2008, S. 200; *Krasilovsky/Shemel*, Music Business, 2007, S. 417.
28 *Schultz*, 43 U. Rich. L. Rev. 685, 689 (2009).
29 *Perritt*, 16 Mich. St. J. Int'l Law 113, 115 (2007); *Schultz*, 43 U. Rich. L. Rev. 685, 690 (2009).
30 *Perritt*, s.o.; s. a. *Krasilovsky/Shemel*, Music Business, 2007, S. 415.
31 Vgl. 7. Kapitel, Teil A.II.2.

jeweiligen Neuerscheinung.[32] Diese erfolgte bis zum Anbruch der Ära des Internets hauptsächlich über drei Kanäle: Einzelhändler, Radio und Musikvideos. Sowohl die Vermarktungsfunktion des klassischen Einzelhändlers[33] als auch diejenige des Mediums Radio[34] wurden jedoch in den letzten Jahren weitgehend ausgehöhlt. Hingegen übernehmen Internetdienste wie Soziale Netzwerke und Videoplattformen in diesem Zusammenhang eine immer wichtigere Funktion. Internetdienste wie YouTube und MySpace Music entwickeln sich zu einem Dreh- und Angelpunkt bei der Vermarktung von Neuerscheinungen, da hier Musikfans die angebotenen multimedialen Inhalte nach neuen Künstlern und Musikrichtungen durchsuchen, favorisierte Inhalte an Freunde weiterempfehlen und auf die Seiten der jeweiligen Künstler und Unternehmen weitergeleitet werden können. Allerdings lassen sich die durch solche Plattformen zu erzielenden Marketingeffekte nur begrenzt steuern, da es in solchen interaktiven Diensten allein die Nutzer sind, die darüber entscheiden, welche Musik sie hören und weiterempfehlen wollen. Tonträgerunternehmen können auf diese Entscheidungen nur begrenzt Einfluss nehmen, beispielsweise dadurch, dass Musikvideos und weitere Information über Neuerscheinungen auf einschlägigen Plattformen den Nutzern zur Verfügung gestellt werden.

c. Schrumpfen des Marktes für physische Datenträger

Weiterhin basierte der Erfolg des Geschäftsmodells der Tonträgerunternehmen bisher darauf, die von ihnen verauslagten Kosten für die Herstellung, den Vertrieb und die Vermarktung einer Tonaufnahme hauptsächlich über die Einnahmen zu decken, die sie mit dem Vertrieb physischer Datenträger erzielten. Darüber hinaus mussten damit die sonstigen Fixkosten sowie die Verluste aus wirtschaftlich nicht erfolgreichen Neuerscheinungen kompensiert werden. Allerdings waren etwa 80 Prozent aller Neuerscheinungen Verlustgeschäfte, d.h. die damit erzielten Einnahmen reichten in der Regel nicht dazu aus, die verauslagten Kosten zu decken.[35] Der wirtschaftliche Erfolg eines Tonträgerunternehmens hing somit maßgeblich von den Einnahmen ab, die durch Tonaufnahmen mit hohen Absatzahlen („Bestseller")

32 *Einhorn*, Gorillas in Our Midst, 2007, S. 2.

33 Beim spezialisierten Einzelhändler konnten sich Musikfans über den in der Regel umfangreichen Musikkatalog sowie die qualifizierte Beratung über neueste Musiktrends und –veröffentlichungen informieren. Einzelhändler wurden jedoch weitgehend von großen Warenhausketten (beispielsweise Wal-Mart) verdrängt, die mittlerweile mehr als die Hälfte aller in den USA verkauften Musikalben vertreiben; vgl. *Krasilovsky/Shemel*, Music Business, 2007, S. 6.

34 Vor allem junge Musikkonsumenten hören kaum mehr Radio zu dem Zweck, sich über neue Musiktrends zu informieren. Das Radio ist zunehmend auf die Rolle eines rein unterhaltenden Begleitmediums reduziert.

35 *Einhorn*, Gorillas in Our Midst, 2007, S. 2-3.

erzielt wurden. In den letzten zehn Jahren hat sich das Gesamtvolumen des mit verkauften Musiktiteln, -alben und -videos zu erzielenden Umsatzes, auch unter Berücksichtigung der zusätzlichen Einnahmen aus dem digitalen Vertrieb von Tonaufnahmen, jedoch stetig verringert, so beispielsweise im Jahr 2008 im Vergleich zum Vorjahr weltweit um 8,5 Prozent.[36] In den USA betrug der Einbruch im Gesamtvolumen in diesem Jahr im Vergleich zum Vorjahr bei 18,6 Prozent, trotz eines Anstiegs um 16,5 Prozent im digitalen Bereich, da beim Absatz physischer Datenträger ein Umsatzrückgang von 31,2 Prozent verzeichnet wurde.[37] In Europa belief sich der Umsatzrückgang auf insgesamt 6,3 Prozent, mit einem Einbruch im physischen Vertrieb von 11,3 Prozent, dem ein Anstieg im digitalen Bereich von 36,1 Prozent gegenüberstand.[38]

Beim Rückgang des Verkaufs physischer Datenträger spielt auch die Internetpiraterie eine Rolle, d.h. die Möglichkeit, digitale Tonaufnahmen im Internet schnell, einfach und kostenlos über illegale Quellen wie beispielsweise internetbasierte Tauschbörsen für digitale Inhalte („Filesharing-Netzwerke") nachzufragen und anzubieten.[39] Dieses Phänomen trägt maßgeblich dazu bei, dass es den Tonträgerunternehmen in den letzten Jahren zunehmend schwer fällt, auf der Grundlage ihres tradierten Geschäftsmodells ihre Kosten zu decken und darüber hinaus Gewinne zu erwirtschaften.[40] Allerdings ist dieser Umsatzeinbruch nicht allein auf die Verbreitung von illegalen Filesharing-Netzwerken zurückzuführen, die den käuflichen Erwerb von CDs überflüssig machen, sondern vor allem auf den Trend, wonach sich die Nachfrage der Musikkonsumenten zunehmend vom physischen Datenträger weg und hin zum Erwerb von Musiktiteln im rein digitalen Format verlagert.[41] Denn Tonaufnahmen werden heutzutage erworben, um sie über verschiedenste digitale Endgeräte, wie beispielsweise Computer, Personal Digital Assistants, Handys oder Smartphones sowohl unterwegs als auch zuhause zu konsumieren.[42] Eine über das Internet erworbene und auf den heimischen Computer heruntergeladene digitale Tonaufnahme kann der Nutzer jedoch sofort auf alle digitalen Endgeräte seiner Wahl übertragen. Erwirbt er hingegen eine Tonaufnahme auf CD, muss er zunächst die Datei von der CD auf den Computer übertragen, bevor er sie von dort aus auf ein anderes Gerät aufspielen kann. Auch ist es weniger

36 Vgl. *IFPI*, Recorded Music Sales 2008; s.a. *Altig/Clement/Papies*, in: *Clement/Schusser/Papies* (Hrsg.), Ökonomie Musikindustrie, 2008, S. 19 ff.
37 Vgl. *IFPI* s.o.
38 Vgl. *IFPI* s.o.
39 Vgl. 3. Kapitel, Teil B.
40 *Schultz*, 43 U. Rich. L. Rev. 685, 690 (2009).
41 So die Unternehmensberatung Pricewaterhouse Coopers, zitiert bei *Bonstein*, Kundensuche im Feindesland, Der Spiegel, 16/2009, S. 100, 101; vgl. auch *Anderson*, Cash for Clicks, The Guardian, 10.8.2009, http://www.guardian.co.uk/media/2009/aug/10/paid-content-charging-online (zuletzt abgerufen am 01.07.2010).
42 *Perritt*, 16 Mich. St. J. Int'l Law 113, 115 (2007).

aufwendig, eine Tonaufnahme als digitale Datei über den heimischen Computer zu erwerben, als zum Zweck des Erwerbs der Tonaufnahme auf CD einen Händler aufsuchen zu müssen oder im Falle der Bestellung über einen Internethändler die gewünschte Tonaufnahme erst mehrere Tage später nach deren Lieferung nutzen zu können.

Die Gewinnspanne beim Vertrieb von Tonaufnahmen in Form von digitalen Downloads fällt jedoch geringer aus als beim Vertrieb über CD. Aufgrund der veränderten Nachfrage der Nutzer schrumpft somit der Markt für den reinen Verkauf von Musiktiteln und –alben insgesamt, da die weniger gewinnträchtigen digitalen Formate die teureren physischen Datenträger mehr und mehr ersetzen.

d. Zusammenfassung

Im Ergebnis bleibt somit festzuhalten, dass sowohl die traditionell von den Tonträgerunternehmen übernommenen Funktionen als auch deren jahrelang praktiziertes Geschäftsmodell durch die Digitalisierung grundsätzlich in Frage gestellt werden.[43] Denn für die erfolgreiche Etablierung eines Musikkünstlers ist nicht länger die Unterstützung durch ein Tonträgerunternehmen unabdingbare Voraussetzung, da der Künstler eine Tonaufnahme mit Hilfe von Computer und entsprechender Software selbst herstellen und über das Internet vertreiben und vermarkten kann. Zudem führt die Internetpiraterie sowie der kontinuierliche Trend beim Konsum von Musik weg von physischen Datenträgern hin zu rein digitalen Formaten dazu, dass Tonträgerunternehmen ihre Kosten im Zusammenhang mit der Produktion, dem Vertrieb und der Vermarktung eines Künstlers nicht mehr allein über den Vertrieb von Tonaufnahmen in Form von physischen Datenträgern decken können. Dies bedeutet jedoch auch, dass im Zeitalter der Digitalisierung, in der die Bindung der Tonaufnahme an einen physischen Datenträger zunehmend bedeutungslos wird, einzig die an einer Tonaufnahme bestehenden urheberrechtlichen Rechtspositionen nachhaltig sind. Denn diese Rechte stellen zum derzeitigen Zeitpunkt, d.h. an der Schnittstelle zwischen dem veralteten Modell des analogen Zeitalters, das auf den Vertrieb physischer Datenträger fokussiert war, und den zukünftig zu definierenden neuen Geschäftsmodellen der digitalen Ära die einzig bleibende und unverrückbare Grundlage dar, um Tonaufnahmen auch in Zukunft kommerzialisieren zu können.[44]

43 *Schultz*, 43 U. Rich. L. Rev. 685, 690 (2009).

44 *Krasilovsky/Shemel*, Music Business, 2007, S. 426: *"In the digital era the only sustainable business advantage is the ownership of the rights to the music itself… ."*.

Die kontinuierliche Fortentwicklung von Komprimierungstechnologien hat auch zu einer massiven Verringerung der Größe von Filmdateien geführt.[45] Allerdings ist eine durchschnittliche auf einer Digital Versatile Disk („DVD"), d.h. auf dem zum Vertrieb von Filmwerken gegenwärtig noch überwiegend verwendeten Datenträger, gespeicherte Filmdatei auch nach der Komprimierung immer noch einige hundert Megabytes groß. Somit ist bei einer Übertragung einer solchen Filmdatei über ein Filesharing-Netzwerk auch zum gegenwärtigen Zeitpunkt noch mit einer Dauer von mehreren Stunden zu rechnen.[46] Vor allem aus diesem Grund ist die Filmindustrie bisher wesentlich weniger stark als die Musikindustrie von den negativen Folgen der Digitalisierung, insbesondere der Internetpiraterie, betroffen. Weiterhin konnte von den Rechtsinhabern für DVDs aufgrund der unmittelbaren Einbettung der insoweit verwendeten DRM-Technologie in jeden DVD-Rohling sowie in jedes zum Abspielen einer DVD befähigten digitalen Endgerätes ein relativ erfolgreiches DRM-System errichtet werden.[47] Darüber hinaus bestehen im Internet nach wie vor nur sehr begrenzte legale Angebote zum Konsum von Filmen und Videos, so dass hieraus dem Vertrieb von Filmen über physische Datenträger noch kein spürbarer (legaler) Wettbewerb erwächst.

Dennoch wird die Übertragung von Filmdateien durch die fortschreitende Verbreitung und Verbilligung von breitbandigen, schnellen Internetzugängen sowie darüber hinaus die Verfügbarkeit hochentwickelter Filesharing-Software, die zunehmend zu einer effizienten Übertragung auch großer Datenmengen in der Lage ist, ständig weiter vereinfacht. Dadurch wird der Konsum von Filmwerken über das Internet für Internetnutzer zunehmend attraktiver.[48] Vor diesem Hintergrund wächst in der Filmindustrie die Angst, dass sie bald ähnlich stark von den negativen Auswirkungen der Digitalisierung betroffen sein könnte wie die Musikindustrie.[49] So wurde beispielweise der Film „Wolverline" innerhalb von 24 Stunden

45 Wie beispielsweise DivX, vgl. *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 20.

46 *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 21; *Anderson*, Cash for Clicks, The Guardian, 10.8.2009, http://www.guardian.co.uk/media/2009/aug/10/paid-content-charging-online (zuletzt abgerufen am 01.07.2010).

47 Vgl. 4. Kapitel, Teil B.III.3.

48 Sogenannte „streaming services", die sich im Musikbereich in Form von Diensten wie beispielsweise last.fm etabliert haben, gelten für den Filmbereich hingegen nach wie vor als unattraktiv, da das Streamen technisch eine hohe Kompression der Filmdatei erfordert, womit Qualitätseinbußen beim Abruf der Datei einhergehen; dies stellt insbesondere ein Problem bei den neuen High-Definition-Formaten wie Blu-ray dar, *Anderson*, Cash for Clicks, The Guardian, 10.8.2009, http://www.guardian.co.uk/media/2009/aug/10/paid-content-charging-online (zuletzt abgerufen am 01.07.2010).

49 *Sandoval*, MPAA: Antipiracy is now „content protection", CNET News, 16.10.2009, http://news.cnet.com/8301-31001_3-10376839-261.html?part=rss&tag=feed&subj=News-DigitalMedia (zuletzt abgerufen am 01.07.2010).

100.000-mal heruntergeladen, nachdem er über eine unbekannte Quelle im April 2009 im Internet verfügbar gemacht worden war.[50] Auch gingen die Einnahmen aus dem Verkauf von DVDs 2009 im Vorjahresvergleich um 13 Prozent zurück, von $10,06 Milliarden auf $8,73 Milliarden Dollar.[51]

B. Das Problem der Internetpiraterie

Die Multimediaindustrie sieht sich in ihren tradierten Strukturen vor allem auch durch das Phänomen der Internetpiraterie bedroht. Hierunter versteht man die Verfügbarkeit von Raubkopien digitaler Multimediawerke – vor allem in Filesharing-Netzwerken – in einem bis zum Anbruch des digitalen Zeitalters unvorstellbaren Ausmaß.[52] Anzumerken ist insoweit, dass auf wissenschaftlicher Ebene jedenfalls umstritten ist, ob und inwieweit die Internetpiraterie für die wirtschaftliche Krise der Multimediaindustrie verantwortlich ist.[53]

I. Einführung

Der wesentliche Unterschied zwischen der Gefahr, die die Internetpiraterie darstellt, und derjenigen, die von Raubkopien in der analogen Welt ausging, liegt darin, dass der großangelegte Vertrieb illegal erstellter Vervielfältigungsstücke von physischen Datenträgern wie CDs und DVDs eine große logistische Herausforderung darstellt. Denn hierfür sind eine organisatorische Infrastruktur, Produktionsstätten und die Etablierung von physischen Vertriebswegen erforderlich und damit erhebliche finanzielle Mittel.[54] Bereits aus diesem Grund stellte im analogen Zeitalter der Schwarzmarkt zu keiner Zeit eine ernsthafte Bedrohung für die Existenzgrund-

50 Vgl. *IFPI*, IFPI Digital Music Report 2010.

51 Allerdings erhöhten sich die Einnahmen aus in den U.S.-amerikanischen Kinos angelaufenen Filmen auf 9,87 Mrd. Dollar und lagen damit sogar 10 Prozent höher als im Vorjahr, weswegen die Filmwirtschaft ingesamt gesehen nur einen mimimalen Umsatzrückgang von 0,3 Prozent erlitt, vgl. *Cheng*, DVD sales tank in 2009 as Americans head to the cinema, Ars Technica, 04.01.2010, http://arstechnica.com/media/news/2010/01/dvd-sales-tank-in-2009-as-americans-head-to-the-cinema.ars (zuletzt abgerufen am 01.07.2010).

52 Bedrohung durch das sogenannte "Darknet", vgl. hierzu *Biddle/England/Peinado/Willman*, The Darknet and the Future of Content Distribution, abrufbar unter http://msl1.mit.edu/ESD10/docs/darknet5.pdf (zuletzt abgerufen am 01.07.2010).

53 Vgl. *Altig/Clement/Papies*, in: *Clement/Schusser/Papies* (Hrsg.), Ökonomie Musikindustrie, 2008, S. 17 m.V.a. entsprechende Studien betreffend den wirtschaftlichen Einfluß der Internetpiraterie auf den Musikmarkt; vgl. hierzu auch den Beitrag von *Becker/Clement/Schusser*, „Piraterie in Peer-to-Peer-Netzwerken, in: *Clement/Schusser/Papies* (Hrsg.), Ökonomie Musikindustrie, 2008,S. 211 ff; vgl. weiterhin *Kouretsidis*, Dgitaler Musikmarkt, 2007, S. 7 mit weiteren Hinweisen auf empirische Studien.

54 *Lincoff*, 2 J. Int'l Media & Ent. L. 1, 4 (2008-2009).

lage der Multimediaindustrie dar. Hingegen ist im Zeitalter der Digitalisierung die Produktion und Verbreitung von Raubkopien von digitalen Multimediawerken schnell, einfach und ohne großen finanziellen Aufwand möglich. So ist fast jeder Internetnutzer unter Nutzung der regulären technischen Fähigkeiten seines Computer und des Internets in der Lage, digitale Multimediawerke zunächst von einer CD oder DVD auf seinen Computer zu übertragen und von hieraus über das Internet an Dritte weiter zu verbreiten.[55]

Zudem bieten Filesharing-Netzwerke Internetnutzern die Möglichkeit, sich mit anderen Nutzern zum Zwecke des Tauschs von Dateien mit Multimediawerken zusammenzuschließen. In einem solchen Netzwerk können die Computer aller Nutzer, die zeitgleich im Netzwerk eingeloggt sind, nach bestimmten digitalen Inhalten durchsucht werden. Wird die von einem Nutzer gesuchte Datei irgendwo im Netzwerk lokalisiert, so kann eine Kopie der Datei über eine Internetverbindung auf den Computer des nachfragenden Nutzers übertragen und dort gespeichert werden. In der Regel basieren Filesharing-Netzwerke auf einer sogenannten „peer-to-peer"-Software. Mit ihrer Hilfe wird ein Netzwerk „unter Gleichen" erstellt, d.h. eine unmittelbare technische Kommunikation zwischen Computern, die die gleichen technischen und funktionellen Voraussetzungen aufweisen.[56] Daten, die innerhalb solcher Filesharing-Netzwerke kommuniziert werden, machen nach einem im Oktober 2009 veröffentlichten Bericht des auf Netzwerkmanagement spezialisierten Unternehmens Sandvine derzeit etwa 20 Prozent des gesamten Datenverkehrs des Internets aus.[57]

II. Der Kampf der Multimediaindustrie gegen die Internetpiraterie

Bei der Bekämpfung des Phänomens der Internetpiraterie verfolgt die Multimediaindustrie mehrere unterschiedliche Strategien, die nachfolgend kurz dargestellt werden.

1. Klagen gegen die Anbieter von Filesharing-Netzwerken und -Technologien

Ein Vorgehen gegen die Anbieter von Filesharing-Netzwerken und Technologien schien zunächst als die praktischste und effizienteste Lösung des Problems der Internetpiraterie. Denn durch die Beseitigung der Netzwerke erhofften sich die

55 *Lincoff*, s.o.; *Roth*, 18 Fordham Intell. Prop. Media & Ent. L.J. 515, 522 (2008).
56 *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 23.
57 *Sandvine*, 2009 Global Broadband Phenomena, S. 2, abrufbar unter http://www.sandvine.com/downloads/documents/2009%20Global%20Broadband%20Phenomena%20-%20Full%20Report.pdf (zuletzt abgerufen am 01.07.2010).

Rechtsinhaber, das Übel an der Wurzel zu packen. Dieser Weg erschien aussichtsreicher als die Durchführung von Klageverfahren gegen Millionen einzelne Nutzer, die im Rahmen solcher Netzwerke illegal Daten tauschen.[58]

Den Auftakt machte in den USA im Jahr 1999 das Verfahren gegen das Unternehmen Napster. Darauf folgten weitere Klagen, u.a. gegen Scour, Aimster, Audiogalaxy, Morpheus, Kazaa, iMesh und LimeWire.[59] Die drei wichtigsten Verfahren dieser sogenannten „dissemination technology cases"[60] gegen Napster, Aimster sowie die Softwareanbieter sowie Grokster/Streamcast werden nachfolgend kurz dargestellt. Denn diese Fälle haben die Beurteilung der Haftung von ISPs für Urheberrechtsverletzungen der Nutzer ihrer Internetdienste, die für die Zwecke dieser Arbeit eine wichtige Rolle spielt,[61] nachhaltig beeinflusst.

a. Napster

In dem Verfahren *A&M Records, Inc. v. Napster Inc.* („Napster") wurde im Dezember 1999 zunächst der ISP Napster, Inc. von mehreren Tonträgerunternehmen wegen Urheberrechtsverletzung („copyright infringement") verklagt.[62]

Der Beklagte vertrieb über das Internet eine kostenlose Software, nach deren Installation sich die Nutzer in das vom Beklagten unterhaltene Netzwerk einloggen und mit anderen, ebenfalls im Netzwerk eingeloggten Nutzern digitale Tonaufnahmen im MP3-Format („Musikdatei") tauschen konnten.[63] Aufgrund der ausgeklügelten Suchfunktionen sowie der sich innerhalb kürzester Zeit entwickelnden extremen Popularität des Netzwerks hatten die Nutzer des Netzwerks bald die Möglichkeit, die Festplatten von Millionen von Nutzern auf Dateien mit ihren Lieblingstiteln hin zu durchsuchen.[64] Die Nutzung des Netzwerks war für die Nut-

58 *Reichman/Dinwoodie/Samuelson*, 22 Berkeley Tech. L.J. 981, 1014 (2007); *Lemley/Reese*, 56 Stan. L. Rev. 1345, 1349 (2004).
59 Vgl. den Bericht der *EFF,* RIAA v. The People, 2008.
60 *Reichman/Dinwoodie/Samuelson*, 22 Berkeley Tech. L.J. 981, 1012 (2007).
61 Vgl. 8. Kapitel.
62 *A&M Records, Inc. v. Napster Inc.*, 114 F. Supp. 2 d 896 (N.D. Cal. 2000).
63 114 F. Supp. 2 d 896, 901.
64 114 F. Supp. 2 d 896, 902. Aus technischer Sicht bestand das Netzwerk des Beklagten aus Gruppierungen von Servern, sog. „Cluster", an die die Nutzer angeschlossen wurden und in der Folge Musikdateien mit denjenigen Nutzern des Netzwerks, die demselben Cluster zugewiesen waren, austauschen konnten. Dabei wurden die Suche und der Austausch der Musikdateien über die Server des Beklagten zentralisiert gesteuert. Sobald sich ein Nutzer im Netzwerk einloggte, stellte der auf dem Computer des Nutzers durch die Software des Beklagten installierte Browser einen Kontakt mit einem Server des Netzwerks her und lud eine Liste der Namen aller der in der Musikbibliothek des Computer des Nutzers vorhandenen

zer kostenfrei, da die Geschäftsstrategie des Beklagten darin bestand, zunächst einen möglich großen Kundenstamm aufzubauen, um diesen zu einem späteren Zeitpunkt zu kommerzialisieren.[65] Von den getauschten Musikdateien entfiel den Untersuchungen der Kläger zufolge ein Anteil von mehr als 80 Prozent auf urheberrechtlich geschützte Musikdateien, deren Nutzung im Rahmen des Netzwerks des Beklagten von den Rechtsinhabern nicht autorisiert worden war.[66]

Der Beklagte stützte seine Verteidigung vor allem auf die vom Supreme Court entwickelte Sony-Doktrin[67] mit dem Argument, dass das von ihm betriebene Netzwerk neben dem Tausch nicht autorisierter digitaler Kopien von Tonaufnahmen auch zu wesentlichen rechtmäßigen Zwecken genutzt werden könne. Dieser Auffassung schloss sich das erstinstanzliche Gericht nicht an, da die vom Beklagten angeführten rechtmäßigen Verwendungsmöglichkeiten im Vergleich zu dem Umfang rechtswidriger Nutzungen kaum ins Gewicht fallen oder nur in Verbindung mit rechtswidrigen Handlungen auftreten würden.[68] Auch könne die Sony-Doktrin aufgrund der zentralen Rolle, die der Beklagte als Betreiber des Netzwerks im Zusammenhang mit den über sein Netzwerk ermöglichten Urheberrechtsverletzungen spielte, keine Anwendung finden.[69] Da die Sony-Doktrin einer Haftung des Beklagten wegen *contributory infringement*[70] somit nicht entgegenstand, kam das Gericht zu dem Ergebnis, dass der Beklagte nach den Grundsätzen dieses Rechtsinstituts für die Urheberrechtsverletzungen seiner Nutzer verantwortlich war. Darüber hinaus sah es auch die Voraussetzungen der *vicarious liability*[71] durch den Beklagten als erfüllt an.[72]

In der Berufungsinstanz bestätigte der Ninth Circuit die Haftung des Beklagten.[73] Abweichend von der Begründung des erstinstanzlichen Gerichts ging der

MP3-Dateien auf den Server hoch. Diese Liste wurde Teil eines durch den Server erstellten, in Echtzeit aktualisierten Gesamtindexes aller Dateinamen, die über die Computer sämtlicher zum gleichen Zeitpunkt eingeloggter Nutzer an den Server kommuniziert worden waren. Diesen Index konnte jeder Nutzer durch Aktivierung der Suchfunktion der Software auf die gewünschten Musikdatei hin durchsuchen, woraufhin der Server dem Nutzer eine Liste derjenigen Dateinamen übermittelte, deren Bezeichnungen mit dem von ihm eingegebenen Suchbegriff übereinstimmten. Forderte der Nutzer hierauf den Download einer dieser Dateien an, fragte der Server des Beklagten bestimmte Informationen über den Computer des Nutzers ab, auf dessen Festplatte sich die angeforderte Datei befand und übermittelte diese an den nachfragenden Computer, der auf dieser Grundlage eine Internetverbindung herstellen und die angeforderte Datei herunterladen konnte.

65 114 F. Supp. 2 d 896, 902.
66 114 F. Supp. 2 d 896, 903.
67 Vgl. 8. Kapitel, Teil B.II.2.b.(bb)(1).
68 114 F. Supp. 2 d 896, 912.
69 114 F. Supp. 2 d 896, 917: *"In any event, Napster's primary role of facilitating the unauthorized copying and distribution established artists' songs renders Sony inapplicable."*
70 Vgl. 8. Kapitel, Teil B.II.2.
71 Vgl. 8. Kapitel, Teil B.II.3.
72 114 F. Supp. 2 d 896, 920-22.
73 *A&M Records, Inc. v. Napster Inc.*, 239 F.3 d 1004 (9th Cir. 2001).

Ninth Circuit jedoch von der grundsätzlichen Anwendbarkeit der Sony-Doktrin auf den Beklagten aus.[74] Das erstinstanzliche Gericht habe bei der Beurteilung der Funktionen des Internetdienstes nicht ausreichend berücksichtigt, dass der Dienst trotz der Tatsache der derzeitigen überwiegenden Nutzung zur Begehung von Urheberrechtsverletzungen seiner technischen Beschaffenheit nach auch zu rechtmäßigen Zwecken verwendet werden könne. Diese theoretische Fähigkeit zur Ausführung rechtmäßiger Funktionen reiche für die Anwendbarkeit der Sony-Doktrin aus. Dennoch wurde der Beklagte auch nach Ansicht des Ninth Circuit hierdurch im Ergebnis nicht vor einer Haftung als *contributory infringer* geschützt. Denn es seien genug Anhaltspunkte dafür gegeben, dass der Beklagte über das generelle Bewusstsein der Möglichkeit der rechtswidrigen Verwendung hinaus auch positive Kenntnis von dem Vorhandensein konkreter rechtswidriger Inhalte in seinem Netzwerk gehabt habe.

b. Aimster

Wenig später wurde in dem Verfahren *In re Aimster Copyright Litigation* („Aimster") auch der Betreiber des Filesharing-Netzwerks Aimster von einigen Tonträgerunternehmen und Musikverlagen wegen der im Rahmen dieses Netzwerks durch die Nutzer begangenen Urheberrechtsverletzungen verklagt.[75] Wie in *Napster* konnten Internetnutzer über das Netzwerk der Beklagten Musikdateien untereinander austauschen.[76] Eine Besonderheit des Netzwerks bestand darin, dass der Prozess der internetbasierten Übertragung der Musikdateien codiert stattfand. Die jeweils auszutauschende Datei wurde somit während des Übermittlungsvorgangs zunächst ver- und erst nach abgeschlossener Übertragung auf den Computer des nachfragenden Nutzers wieder entschlüsselt.

Bereits das erstinstanzliche Gericht war zu dem Ergebnis gekommen, dass die Beklagten für die im Rahmen ihres Netzwerks stattfindenden Urheberrechtsverletzungen der Nutzer nach den Grundsätzen des *contributory infringement* hafteten und untersagte den Beklagten den fortgesetzten Betrieb ihres Netzwerks. In der

74 239 F.3 d 1004, 1020-22.

75 *In re Aimster Copyright Litigation*, 252 F. Supp. 2 d 634 (N.D. Ill. 2002).

76 Technisch basierte das Netzwerk der Beklagten auf der Ausnutzung der Funktionen von sog. Instant-Messaging-Diensten („IM-Dienst") wie beispielsweise demjenigen des Internetdienstes AOL. Voraussetzung für die Nutzung des Netzwerks der Beklagten war somit die gleichzeitige Nutzung eines solchen IM-Dienstes, da für den Austausch von Musikdateien die gleichzeitige Anwesenheit der tauschenden Nutzer in einem sogenannten „Chat-Raum" notwendig war. Um das Netzwerk nutzen zu können, mussten zunächst eine kostenlose, auf der Webseite der Beklagten zur Verfügung gestellte Software heruntergeladen werden. Nach Installation der Software und Anmeldung im System anhand Nutzername und Passwort konnten die Nutzer jeden anderen im System registrierten Nutzer zu ihren „Buddies" erklären, mit denen sie dann direkt kommunizieren und Musikdateien austauschen konnten.

dagegen eingelegten Berufung bestätigte der Seventh Circuit[77] die Entscheidung des erstinstanzlichen Gerichts. Die Sony-Doktrin sei trotz des Umstandes, dass der Dienst des Beklagten theoretisch auch zu rechtmäßigen Zwecken verwendet werden könne, nicht anwendbar, da die Beklagten Beweise dafür schuldig geblieben seien, dass ihr Dienst jemals tatsächlich zu einem solchen rechtmäßigen Zweck genutzt worden wäre.[78] Auch scheitere die Haftung der Beklagten wegen *contributory infringement* nicht daran, dass sie aufgrund der Verschlüsselungsfunktion nicht wussten, welche Dateien im Rahmen des Netzwerks von den Nutzern getauscht wurden, und damit keine positive Kenntnis von den Rechtsverletzungen hatten. Insoweit müsse berücksichtigt werden, dass die Beklagten selbst die Verschlüsselungsfunktion freiwillig in das Netzwerk eingeführt und somit ihre Unkenntnis selbst verschuldet hatten, weswegen die auf dieser Weise herbeigeführte Unkenntnis sie nicht vor der Haftung bewahren könne.

c. Grokster

Das Verfahren *MGM Studios, Inc. v. Grokster Ltd.* („Grokster"), das von den großen Hollywoodstudios[79] und einigen anderen Unternehmen der Multimediaindustrie gegen die Filesharing-Dienste Grokster Ltd. und Streamcast Networks Inc. angestrengt wurde, gelangte schließlich bis vor den Supreme Court.[80]

Im Unterschied zu *Napster* und *Aimster* waren die Beklagten in *Grokster* an den Aktivitäten der Nutzer im Zusammenhang mit den durch ihre Software errichteten Netzwerken nicht unmittelbar involviert, d.h. deren Server übernahmen keinerlei Funktion bei der Suche nach urheberrechtlich geschützten digitalisierten Inhalten und deren Übertragung.[81] Der einzige unmittelbare Kontakt zwischen den Beklag-

77 *In re Aimster Copyright Litigation*, 334 F.3 d 643 (7th Cir. 2003).
78 334 F.3 d 643, 651.
79 Metro-Goldwyn-Mayer Studios, Inc., Columbia Pictures Industries, Inc., Disney Enterprises, Inc., Paramount Pictures Corporation; Twentieth Century Fox Film Corporation und Universal City Studios LLP.
80 *MGM Studios, Inc. v. Grokster Ltd.*, 545 U.S. 913 (2005).
81 Die über das Internet vertriebene Software basierte im Falle von Grokster auf der sog. Fast-Track-Technologie und im Falle von Streamcast auf der sog. Gnutella-Technologie. Beide Technologien ermöglichten es ihren Nutzern, bei der Suche nach Dateien mit bestimmten digitalen Inhalten direkte Anfragen an die Computer anderer, die gleiche Software verwendende Nutzer zu senden. Im Rahmen der Fast-Track-Technologie wurde eine solche Suchanfrage an einen sog. „Supernode" übermittelt, d.h. an einen Computer, der über die Fähigkeit zur Indexierung von auf den mit ihm verbundenen Computern gespeicherten Dateien verfügte und die Suchanfrage zudem an andere Supernodes weiterleitete. Nachdem ein Supernode die gesuchte Datei auf einem Computer lokalisiert hatte, teilte er dies dem Computer des suchenden Nutzers mit, der auf Grundlage dieser Information eine unmittelbare Verbindung

ten und den Nutzern der Filesharing-Netzwerke bestand darin, dass die Nutzer die von den Beklagten im Internet zur Verfügung gestellte Software von deren Webseiten auf ihre Computer herunterladen mussten, bevor sie die Filesharing-Netzwerke nutzen konnten. Aufgrund dieser dezentralen Struktur der von den Beklagten angebotenen Netzwerke hatten sowohl das erstinstanzliche Gericht als auch der Ninth Circuit eine Haftung der Beklagten für die Urheberrechtsverletzungen der Nutzer abgelehnt.[82]

Hingegen entschied der Supreme Court unter Heranziehung des patentrechtlichen Grundsatzes der Haftung für schuldhafte Veranlassung („inducement rule"),[83] dass die Beklagten für die Urheberrechtsverletzungen der Nutzer hafteten. Nach seiner Auffassung hatte der Ninth Circuit die Sony-Doktrin zu weit interpretiert und daher das Vorliegen der subjektiven Voraussetzung der Haftung der Beklagten als *contributory infringer* zu Unrecht verneint. Die Sony-Doktrin besage nur, dass eine Haftung für *contributory infringement* aufgrund von vermutetem Vorsatz („imputed intent") nicht allein darauf gestützt werden könne, dass sich der Hersteller oder Verkäufer einer Technologie bewusst sei, dass die Technologie unter anderem auch zu rechtswidrigen Zwecken eingesetzt werden könne.[84] Darüber hinaus seien die Gerichte jedoch durch die Doktrin nicht daran gehindert, die Haftung auf andere, von dem bloßen Bewusstsein der rechtswidrigen Verwendungsmöglichkeit unabhängige Umstände zu stützen. Die Sony-Doktrin stehe dementsprechend der Bejahung der Haftung für *contributory infringement* nicht entgegen, falls den Beklagten aufgrund anderer Tatsachen eine rechtswidrige Gesinnung nachgewiesen werden könne.[85] Im Falle der Beklagten kam eine solche rechtswidrige Absicht nach Auffassung des Supreme Court jedoch in drei Umständen deutlich zum Ausdruck:

zu dem Computer mit der gesuchten Datei zwecks Übertragung dieser Datei aufbaute. Die Gnutella-Technologie von StreamCasts basierte hingegen nicht auf Supernodes, sondern der Computer des suchenden Nutzer übermittelte dessen Suchanfrage unmittelbar an die mit ihm über die Gnutella-Software verbundenen Computer, die auf die Anfrage antworteten und diese zudem an weitere, mit ihnen verbundene Computer weiterleiteten. Nach Erhalt der Rückmeldungen auf die Anfrage stellte wiederum der Computer des suchenden Nutzers zum Zwecke der Datenübermittlung eine unmittelbare Verbindung zu dem Computer her, auf dem sich die gesuchte Datei befand.

82 *MGM Studios, Inc. v. Grokster, Ltd.*, 380 F.3 d 1154, 1166 (9th Cir. 2003): *"As to the question at hand, the district court's grant of partial summary judgment to the Software Distributors is clearly dictated by applicable precedent. The Copyright Owners urge a re-examination of the law in the light of what they believe to be proper public policy, expanding exponentially the reach of the doctrines of contributory and vicarious copyright infringement. Not only would such a renovation conflict with binding precedent, it would be unwise. Doubtless, taking that step would satisfy the Copyright Owners' immediate economic aims. However, it would also alter general copyright law in profound ways with unknown ultimate consequences outside the present context."*.

83 Vgl. 8. Kapitel, Teil B.II.4.

84 545 U.S. 913, 933-34.

85 545 U.S. 913, 934-35.

(1) Dem Ziel, das Erbe des mittlerweile eingestellten Internetdienstes Napster anzutreten und dessen frühere Nutzer anzuwerben. Dieses Ziel sah der Supreme Court in externer und interner Kommunikation der Beklagten manifestiert.

(2) Den fehlenden Bemühungen der Beklagten, die Rechtsverletzungen der Nutzer im Rahmen des technisch Machbaren einzudämmen, beispielsweise durch den Einsatz von Filtertechnologien.

(3) Dem werbefinanzierten Geschäftsmodell der Beklagten, wonach die Einnahmen der Beklagten von der Menge an bei den Nutzern abgesetzten Werbebotschaften abhängig waren. Deswegen habe es im Interesse der Beklagten gelegen, die Attraktivität des Dienstes für neue Nutzer insbesondere auch durch den ungehinderten Zugang zu urheberrechtlich geschützten Inhalten zu erhöhen.[86]

2. Klagen gegen Einzelpersonen

Neben den Klagen gegen die Anbieter von Filesharing-Netzwerken und –Software ging die Recording Industry Association of America („RIAA“) in den Jahren 2003 bis 2009 in mehr als 30.000 Fällen mit Abmahnungen und Klagen wegen Urheberrechtsverletzungen gegen Einzelpersonen vor, denen vorgeworfen wurde, Musikdateien über Filesharing-Netzwerke getauscht zu haben.[87] In der weit überwiegenden Zahl wurden die US-amerikanischen Verfahren im Wege des Vergleichs gegen Zahlung einer Summe von ca. USD$3.000 bis USD$5.000 durch die Beklagten an die RIAA beendet. In einigen Fällen wurden die Klagen jedoch auch vor Gericht ausgetragen, wie beispielsweise das Verfahren gegen eine alleinerziehende Mutter von zwei Kindern, die zunächst in erster Instanz zu einer Zahlung von USD$222.000 Schadensersatz verurteilt wurde. In der dagegen eingelegten Berufung wurde das Urteil aufgehoben und das Verfahren an das erstinstanzliche Gericht zurückverwiesen. Daraufhin wurde die Beklagte im neuen Verfahren zur Zahlung einer noch um ein Vielfaches höheren Summe von USD$1,92 Millionen verurteilt, was einem Schadensersatz in Höhe von USD$80.000 pro getauschten Musiktitel entspricht.[88]

86 545 U.S. 913, 939-40.

87 *EFF,* RIAA v. The People, 2008; vgl. hierzu auch *Hughes*, 22 Cardozo Arts & Ent. L.J. 725-766 (2005); *Borland*, RIAA Sues 717 File-Swappers, CNET News, 27.1.2005, http://news.com.com/2110-1027_3-5553517.html (zuletzt abgerufen am 01.07.2010).

88 *Harvey*, Single-mother digital pirate Jammie Thomas-Rasset must pay $ 80,000 per song, Times Online, 19.6.2009, http://technology.timesonline.co.uk/tol/news/tech_and_web/article6534542.ece (zuletzt abgerufen am 30.04.2009).

Ende 2008 verkündete die RIAA jedoch, ihre Kampagne gegen Privatpersonen einzustellen und lediglich bereits anhängige Verfahren weiterzuverfolgen.[89] Darin wurde ein Eingeständnis der Musikindustrie gesehen, dass die Klagewelle wenig gegen das Problem der Internetpiraterie auszurichten vermocht hatte[90] und darüber hinaus das Image der Tonträgerindustrie beschädigt hatte,[91] da die Initiative sogar vor Schülern und Studenten keinen Halt gemacht hatte.[92] Hingegen begründete die RIAA die Einstellung ihrer Kampagne damit, dass man sich auf den neuen, vielversprechenderen Ansatz der sogenannten „Graduated Response"[93] zur Bekämpfung der Internetpiraterie konzentrieren wolle.[94]

Auch in Deutschland ist die Musikindustrie seit dem Jahr 2004 dazu übergegangen, Privatpersonen für den illegalen Tausch von Musikdateien über das Internet rechtlich zu verfolgen.[95] Dies führte in Deutschland vor allem deswegen zu heftigen Diskussionen, weil die Musikunternehmen, um an die Identität der Nutzer zu kommen, die über Filesharing-Netzwerke Musikdateien getauscht hatten, zunächst den Umweg über die Strafverfolgungsbehörden[96] nehmen mussten, da ihnen kein selbständiger Auskunftsanspruch gegen die Netzwerkbetreiber zustand. Dies führte dazu, dass die Staatsanwaltschaften mit Strafanzeigen gegen Filesharer geradezu überschwemmt wurden. Im Rahmen des Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums[97] hat der Gesetzgeber jedoch nunmehr in § 101 Abs. 2 UrhG einen eigenen Auskunftsanspruch der Rechtsinhaber gegen die Betreiber von Filesharing-Netzwerken eingeführt.

Offiziell hat die Entscheidung der RIAA, in den USA keine neuen Klagen gegen Privatpersonen mehr anzustrengen, keinen unmittelbaren Einfluss auf die Strategie

89 *Heise Online*, US Musikindustrie gibt Massenklagen auf, 19.12.2008, http://www.heise.de/newsticker/meldung/US-Musikindustrie-gibt-Massenklagen-auf-Update-191425.html (zuletzt abgerufen am 01.07.2010).

90 *McDermott*, The great copyright debate, Managing Intellectual Property, March 2009, S. 26, 29; *EFF,* RIAA v. The People, 2008.

91 *Lincoff*, 2 J. Int'l Media & Ent. L. 1, 5 (2008-2009); s.a. *Krasilovsky/Shemel*, Music Business, 2007, S. 415*: "The situation is complicated by the fact that these "users" are both new competitors and customers of the existing industry. The contradictions implicit in using litigation against your own customer made this a difficult decision, but in the end the threat from individual action was deemed too significant to ignore."*

92 *Harmon*, Recording Industry Goes After Students Over Music Sharing, The New York Times, 23.4.2003, S. A1; *McDermott*, The great copyright debate, Managing Intellectual Property, March 2009, S. 26, 27.

93 Vgl. 3. Kapitel, Teil B.II.3.b.

94 *Heise Online*, US-Musikindustrie: Das Ende der „Schreckensherrschaft"?, heise online, 20.12.2008, http://www.heise.de/newsticker/meldung/120789 (zuletzt abgerufen am 01.07.2010).

95 Vgl. zu einer Darstellung dieser Strategie den Eintrag zum Thema „Internetpiraterie" auf der Webseite des Bundesverbands der Musikindustrie, abrufbar unter http://www.musikindustrie.de/internetpiraterie/ (zuletzt abgerufen am 01.07.2010).

96 Durch Erstattung von Strafanzeige und daraufhin beantragte Einsichtnahme in die Ermittlungsakten.

97 G. v. 7.7.2008, BGBl. I S. 1191.

der Musikindustrie in Deutschland, d.h. Klagen gegen Privatpersonen werden in Deutschland wohl auch in Zukunft fortgeführt werden.[98] Jedoch stellen solche Massenverfahren inzwischen auch nach Einschätzung des deutschen Bundesverbandes Musikindustrie nurmehr „Notwehrlösungen" dar in Ermangelung anderer effektiver Alternativen zur Ahndung und Eindämmung der Internetpiraterie.[99]

3. Aktuelle Entwicklungen

a. BitTorrent

Filesharing-Netzwerke beruhen heutzutage auf Open Source Software oder offenen Protokollen und sind damit weitgehend unabhängig von der Verbreitung und Unterhaltung durch einen bestimmten Software-Anbieter.[100] Dadurch ist es noch schwieriger geworden, gegen Filesharing-Netzwerke vorzugehen.

Ein Beispiel für ein offenes Protokoll ist die sogenannte „BitTorrent"-Technologie. Dieses kollaboratives Filesharing-Protokoll hat es innerhalb kurzer Zeit zu großer Beliebtheit gebracht, da mit seiner Hilfe eine schnellere und effizientere Übertragung auch großer Datenmengen ermöglicht wird.[101] Dieses Protokoll setzt im Gegensatz zu anderen Filesharing-Technologien zur Verteilung der Daten nicht auf ein übergreifendes Filesharing-Netzwerk, sondern errichtet für jede zu übertragende Datei ein eigenes Verteilnetz. Seine Stärke liegt darin, dass die jeweils zu übertragende Datei in einzelne, kleine Einheiten zerlegt und sodann von mehreren Quellen aus an denjenigen, der die Datei angefordert hat, übertragen und auf dessen Computer wieder zusammengesetzt wird. Zu diesem Zweck versieht das Protokoll die auf einem Computer befindlichen Dateien mit einem sogenannten „torrent", einer kleinen Datei, die Informationen über ihre Trägerdatei sowie den sie speichernden Computer enthält.[102] Auf diese Weise markierte Dateien („Torrent-Dateien") können von anderen Nutzern des Protokolls aufgespürt und als Quelle zur Übertragung einzelner Einheiten dieser Dateien auf ihre Computer genutzt werden. Sobald ein Nutzer eine Torrent-Datei auf seinen Computer herunterlädt, kann diese

98 *von Gehlen*, Warnen statt Klagen: Die Musikindustrie ändert ihre Strategie in Sachen Internet-Piraterie, jetzt.de, 23.12.2008, http://jetzt.sueddeutsche.de/texte/anzeigen/459154 (zuletzt abgerufen am 01.07.2010).

99 *Bundesverband der Musikindustrie*, Deutsche Musikindustrie begrüßt geplante Vereinbarung mit US-Providern zur Bekämpfung von Internetpiraterie, 19.12.2008, http://www.musikindustrie.de/presse_aktuell_einzel/back/82/page/5/news/deutsche-musikindustrie-begruesst-geplante-vereinbarung-mit-us-providern-zur-bekaempfung-von-internetpi/ (zuletzt abgerufen am 01.07.2010).

100 Vgl. *EFF,* RIAA v. The People, 2008.

101 *Martin*, 28 Loy. L.A. Ent. L. Rev. 265, 289 (2008).

102 *BitTorrent*, FAQ – BitTorrent Concepts, What is BitTorrent, http://www.bittorrent.com/btusers/help/faq/bittorrent-concepts#4n5 (zuletzt abgerufen am 01.07.2010).

Kopie der Torrent-Datei wiederum als Bezugsquelle für andere Nutzer dienen, wodurch die Anzahl der Anbieter dieser Datei ständig steigt und sich dementsprechend deren Übertragungsprozess ständig beschleunigt. Ein weiterer Vorteil des Protokolls liegt darin, dass sich durch die Aufspaltung der Torrent-Dateien das jeweils durch einen Nutzer innerhalb eines Übertragungsnetzwerks in Anspruch genommene Datenvolumen verringert, was wiederum zur Schnelligkeit der Übertragung beiträgt.

Darüber hinaus erstellt das Protokoll selbst jedoch keine Listen von im Internet zu einem bestimmten Zeitpunkt verfügbaren Torrent-Dateien, anhand derer die Nutzer gezielt nach bestimmten Multimediawerken suchen könnten. Diese Funktion übernehmen sogenannte Torrent-Tracker-Dienste, d.h. Internetdienste, die die vorhandenen Torrent-Dateien indexieren und auf diese Weise eine gezielte Suche nach Dateien mit bestimmten Inhalten unterstützen. Der derzeit populärste Dienst dieser Art ist The Pirate Bay mit Sitz in Schweden.[103]

b. Graduated Response

Ziel der sogenannten „Graduated Response" oder „Three Strikes Policy" ist es, Anbieter von Internetzugängen („Access-Provider") dazu zu verpflichten, Nutzer zu identifizieren, die die ihnen zur Verfügung gestellte Internetverbindung zum illegalen Tausch von digitalen Multimediawerken missbrauchen, sie zu verwarnen und ihnen zeitweise den Internetzugang zu sperren, sofern sie trotz eines wiederholten Hinweises auf die Urheberrechtswidrigkeit ihres Verhaltens dieses nicht einstellen.[104]

103 Vgl. die Informationen des Internetinformationsdienstes *Alexa Internet* zu „thepiratebay.org – The Pirate Bay", http://www.alexa.com/siteinfo/thepiratebay.org (zuletzt abgerufen am 01.07.2010). Zum schwedischen Gerichtsverfahren gegen The Pirate Bay vgl. beispielsweise *Heise Online*, Pirate Bay: Provider kriegen Probleme, 6.10.2009, http://www.heise.de/newsticker/meldung/Pirate-Bay-Provider-kriegen-Probleme-813843.html (zuletzt abgerufen am 01.07.2010).

104 *IFPI,* Digital Music Report 2009, S. 2: *„The vast growth of unlawful file-sharing quite simply threatens to put the whole music sector out of business. This report reflects the wide consensus, from major and independent record companies to managers and politicians, that a new approach is needed to protect copyright – one that involves sharing responsibility across the value chain. The debate has a huge way to go, but the campaign for ISPs to act as proper partners in helping protect intellectual property is making progress. Governments are beginning to understand the scale of the challenge of trying to monetise content in an environment where around 95 per cent of all music is downloaded without payment to artists or producers. France is leading the drive towards ISP cooperation, understanding that it is the future of French creative industries that are at stake. The UK and a growing number of countries have progressed along a similar route in 2008 and momentum will build further in 2009".*

Den größten Erfolg in diesem Zusammenhang konnte die Musikindustrie bisher in Frankreich verbuchen, wo es gelang, den Ansatz der Graduated Response in Form des sogenannten „Loi HADOPI" auch gesetzlich zu verankern. Dieses Gesetz wurde im zweiten Anlauf im September 2009 von der Assemblée Nationale verabschiedet.[105] Demnach kann Nutzern, die wegen der wiederholten Verletzung von Urheberrechten auffallen, der Zugang zum Internet nach zweimaliger vorheriger Verwarnung gesperrt werden. Darüber hinaus drohen ihnen Geld- und sogar Gefängnisstrafen.[106] Über die Verhängung der Sperre oder einer weiteren Sanktion entscheidet ein Richter im abgekürzten Verfahren.[107]

Ob es in den USA, Deutschland oder auf der Ebene der Europäischen Union („EU") zu ähnlichen, erfolgreichen Gesetzesinitiativen wie in Frankreich kommen wird, ist zum gegenwärtigen Zeitpunkt noch nicht endgültig absehbar. Derzeit scheint die Tendenz in Deutschland noch dahin zu gehen, die Einführung eines solchen Gesetzes aus verfassungs- und datenschutzrechtlichen Bedenken grundsätzlich abzulehnen, da die Nutzung von Daten über den Telekommunikationsverkehr zum Zwecke der Versendung von Warnhinweisen sowie gegebenenfalls zur Sperrung von Internetanschlüssen auf eine „Vorratsdatenspeicherung im großen Stil" zur Durchsetzung der privaten Interessen der Rechtsinhaber hinauslaufen würde.[108] Allerdings haben sich die Unterhändler der EU-Mitgliedstaaten, des Europäischen Parlaments und der Europäischen Kommission im November 2009 im Rahmen der Verhandlungen über das Telekom-Novellierungsgesetz auf den Wortlaut einer „neuen Regelung zur Internetfreiheit" („Internet Freedom Provision") geeinigt. Demnach sind Internetsperren, wie sie beispielsweise das Loi HADOPI vorsieht, grundsätzlich zulässig, sofern sie im Rahmen eines fairen und rechtmäßigen Verfahrens ergehen, in dem insbesondere die Anhörung des Betroffenen sowie die zeitnahe gerichtliche Überprüfung einer gegen ihn erlassenen

105 Der Text des Gesetzes ist abrufbar unter http://www.assemb*Lee*-nationale.fr/13/ta/ta0337.asp (zuletzt abgerufen am 01.07.2010).

106 *Heise Online*, Frankreich: Internetsperre für Urheberrechtsverletzer gebilligt, 22.10.2009, http://www.heise.de/newsticker/meldung/Frankreich-Internetsperre-fuer-Urheberrechtsverletzer-gebilligt-837138.html (zuletzt abgerufen am 01.07.2010).

107 In der ursprünglichen Version sollte eine Verwaltungsbehörde über die Verhängung von Sanktionen entscheiden; dagegen erhob jedoch das oberste französische Gericht verfassungsrechtliche Bedenken und kippte den ursprünglichen Gesetzesentwurf.

108 Interview mit Brigitte Zypries, promedia 8/2009, S. 8, 9, http://www.promedia-berlin.de/fileadmin/Archiv/2009/08/promedia200908-online01.pdf (abgerufen am 01.07.2010); auch der Koalitionsvertrag der CDU/CSU/FDP für die neue Legislaturperiode sieht kein solches Modell vor, vgl. *Heise Online*, Schwarz-Gelb gegen Internetsperren bei Urheberrechtsverletzungen, 19.10.2009, http://www.heise.de/meldung/Schwarz-Gelb-gegen-Internetsperren-bei-Urheberrechtsverletzungen-832715.html (zuletzt abgerufen am 01.07.2010); vgl. zur Entwicklung auf EU-Ebene *Heise Online*, Widerstand im EU-Parlament gegen Internet-Sperren bei Urheberrechtsverletzungen bröckelt, 15.10.2009, http://www.heise.de/newsticker/meldung/Wi*der*stand-im-EU-Parlament-gegen-Internet-Sperren-bei-Urheberrechtsverletzungen-broeckelt-830015.html (zuletzt abgerufen am 01.07.2010).

Maßnahme gewährleistet ist.[109] Damit enttäuschte die Internet Freedom Provision diejenigen, die gehofft hatten, dass die EU der Graduated Response eine klare Absage erteilen würde.[110]

III. Zusammenfassung

Es bleibt somit festzuhalten, dass die Multimediaindustrie im Kampf gegen die Internetpiraterie mehrere unterschiedliche Strategien verfolgt. Allerdings hat keine dieser Strategien bisher zu einem durchschlagenden Erfolg geführt, d.h. den Umfang der Internetpiraterie maßgeblich verringert.[111] Vielmehr verzeichnet gerade der Filmbereich einen merklichen Anstieg illegaler Downloads von urheberrechtlich geschützten Filmen.[112]

C. Zwischenergebnis

Der technische Fortschritt des digitalen Zeitalters hat dazu geführt, dass jeder durchschnittliche Nutzer von Computer und Internet Multimediawerke schnell und ohne übermäßigen finanziellen Aufwand digitalisieren, speichern, bearbeiten und an Dritte übermitteln kann.[113] Umgekehrt kann jeder Nutzer digitale Multimediawerke unter Nutzung von Computer und Internet von anderen Nutzern beziehen.

109 MEMO/09/491 v. 5.11.2009: *„The new Internet Freedom Provision - Article 1(3)a of the new Framework Directive: Measures taken by Member States regarding end-users' access to or use of services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law. Any of these measures regarding end-users' access to or use of services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law, including effective judicial protection and due process. Accordingly, these measures may only be taken with due respect for the principle of presumption of innocence and the right to privacy. A prior fair and impartial procedure shall be guaranteed, including the right to be heard of the person or persons concerned, subject to the need for appropriate conditions and procedural arrangements in duly substantiated cases of urgency in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms. The right to an effective and timely judicial review shall be guaranteed.".*

110 *Klopp*, EU lässt Netzsperren zu, Zeit Online, 12.11.2009, http://www.zeit.de/digital/internet/2009-11/eu-netzsperren (zuletzt abgerufen am 01.07.2010).

111 Vgl. *Bernstein/Sekine/Weissman*, Global Music Industry, 2007, S. 9.

112 Vgl. 5. Kapitel, Teil D.III.

113 So auch *Fetscherin*, in: *Becker/Buhse/Günnewig/Rump (Hrsg.),* DRM, 2003, S. 301.

Die Nutzer sind damit zugleich Anbieter und Nachfrager von Multimediawerken geworden. Dies bedeutet jedoch eine Zäsur in Bezug auf die traditionelle Wertschöpfungskette, deren Profiteur am Ende bisher immer die Multimediaindustrie war.

Der Nutzer muss somit zum Zwecke des Bezuges von Multimediawerken nicht mehr notwendigerweise auf die von der Multimediaindustrie kontrollierten Vertriebswege zurückgreifen und hierüber ein Entgelt an die Rechtsinhaber entrichten.[114] Im digitalen Umfeld ist daher nicht mehr sichergestellt, dass die Nutzer in jedem Einzelfall für die Nutzung und den Erwerb von Multimediawerken zahlen. Fällt diese finanzielle Gegenleistung jedoch weg, entfällt damit gleichzeitig die bisherige Grundlage für die Kompensation der Kosten für Produktion und Marketing von Multimediawerken, die von der Multimediaindustrie nach wie vor vorfinanziert werden. Darin liegt die grundsätzliche Bedrohung der Existenzgrundlage der Multimediaindustrie.

4. Kapitel: Technische, ökonomische und rechtliche Grundlagen des Einsatzes von DRM-Systemen

Eine Untersuchung von DRM-Systemen aus juristischer Perspektive kommt nicht umhin, sich zunächst mit den technischen Grundlagen, auf denen DRM-Systeme basieren, sowie dem ökonomischen Kontext, in dem sie eingesetzt werden, zu befassen.[115]

A. Definition des Begriffs „Digital Rights Management"

Im weitesten Sinne wird unter dem Begriff Digital Rights Management die allgemeine Verwaltung von Rechten im digitalen Umfeld verstanden, d.h. die Beschreibung, die Identifikation, der Vertrieb und der Schutz digitaler, urheberrechtlich geschützter Multimediawerke sowie die Überwachung und Nachverfolgung jeglicher in Bezug auf ein solches Werk vorgenommenen Nutzungshandlungen.[116] Im engeren Sinne bezieht sich der Begriff hingegen nur auf die „digital gesteuerte

114 Sogenannte „desegregation of the value chain", vgl. *Fetscherin*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 301, 302.

115 *Rump* vergleicht die drei Säulen (Technologie, Ökonomie und Recht), auf denen DRM ruht, mit einem dreibeinigen Stuhl, der aus dem Gleichgewicht gerät, wenn auch nur eines seiner drei Beine nicht im Einklang mit den anderen beiden steht, vgl. *Rump*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 3, 5.

116 *Rump*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 3, 4; *Arlt*, DRMS, 2006, S. 9.

Verwaltung von Rechten", d.h. die Option, die einem Rechtsinhaber an einem Multimediawerk zustehenden Rechte im digitalen Umfeld mit Hilfe von Technologien zu verwalten,[117] d.h. diese Rechte sowie die Regeln, denen der Rechtsinhaber die Nutzung seines Werks auf der Grundlage seiner Rechte unterwirft, gegenüber dem Nutzer auf technischem Wege durchzusetzen. Im Rahmen dieser engeren Definition steht somit die Bekämpfung von Gefahren, die mit der Digitalisierung für die Durchsetzung von Rechtspositionen einhergehen, durch Technologien im Vordergrund, frei nach Clarks Motto „the answer to the machine is in the machine".[118] Im Rahmen dieser digital gesteuerten Verwaltung von Rechten stellen DRM-Systeme das technische Instrumentarium dar, das den Rechtsinhaber dazu in die Lage versetzt, auch nach der Lieferung des digitalisierten Werks an einen Nutzer „aktives Rechtemanagement" zu betreiben, d.h. die Handlungen des Nutzers in Bezug auf das Werk zu kontrollieren und gegebenenfalls zu unterbinden.[119]

In Bezug auf die Funktionen von DRM-Systemen, die die technologisch gesteuerte Rechteverwaltung im Sinne des engeren Begriffsverständnisses von DRM ermöglichen, ist weiterhin zwischen DRM-Systemen der ersten und zweiten Generation zu unterscheiden. Während DRM-Systeme der ersten Generation ihrem Zweck nach vor allem auf die Verhinderung der Vervielfältigung digitaler Multimediawerke gerichtet waren,[120] bedient die Nachfolgegeneration ein wesentlich größeres Funktionenspektrum.[121] Neben der Verhinderung von seitens des Rechtsinhabers nicht zugelassenen Nutzungshandlungen kann mithilfe solch fortentwickelter, vielschichtiger DRM-Systeme beispielsweise die Identifikation und Nachverfolgung von Multimediawerken im digitalen Umfeld, sowie die individuelle Abrechnung zulässiger Nutzerhandlungen erreicht werden. Solchermaßen eingesetzt wird durch DRM-Systeme die individuelle Vergabe und Abrechnung von Rechten an digitalen Multimediawerken ermöglicht,[122] so dass DRM-Systeme gleichsam als elektronische Lizenzierungssysteme fungieren.[123]

Diese teilweise sehr unterschiedlichen Funktionen werden dadurch erreicht, dass innerhalb des jeweils verwendeten DRM-Systems eine Kombination unterschiedlicher Technologien[124] zum Einsatz kommt. So werden beispielsweise zu

117 *Rump*, s.o.; *Arlt*, DRMS, 2006, S. 10.
118 *Clark*, in: *Hugenholtz* (Hrsg.), The Future of Copyright in a Digital Environment, 1996, S. 139 ff.
119 *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 34; *Schulz*, GRUR 2006, 470, 471; *Arlt*, GRUR 2004, 548, 549; *Bechtold*, DRM, 2002, S. 3 ff.; vgl. auch *Hansen*, Gesprengte Ketten – Legale MP3-Downloads in Deutschland, c't 2009, Heft 9, S. 139.
120 *Grimm*, in: *Roßnagel*, Digitale Rechteverwaltung, 2009, S. 15.
121 *Ünlü*, Content Protection, 2005, S. 48.
122 *Bechtold*, DRM, 2002, S. 2-3; *Roßnagel*, in: *Roßnagel*, Digitale Rechteverwaltung, 2009, S. 15.
123 *Arlt*, DRMS, 2006, S. 11.
124 Vgl. 4. Kapitel, Teil B.II.

Identifikationszwecken, d.h. zur Feststellung, ob ein digitales Multimediawerk bestimmten Rechten Dritter unterliegt, wem diese Rechte zustehen und welchen Umfang diese Rechte haben, vorwiegend sogenannte „rights expression languages" eingesetzt.[125] Im Zusammenhang mit der Verhinderung des unerlaubten Zugriffs und der unerlaubten Nutzung eines digitalisierten Multimediawerks spielen hingegen Verschlüsselungstechnologien eine wichtige Rolle.[126]

In der nachfolgenden Darstellung ist unter dem Begriff DRM bzw. DRM-Systeme durchweg die technologisch gesteuerte Verwaltung und Sicherung von Rechten und Nutzungsbedingungen im Zusammenhang mit digitalen Multimediawerken zu verstehen, d.h. DRM im engeren Sinne. Darüber hinaus bezieht sich der Begriff vor allem im Rahmen der Ausführungen zum Scheitern von DRM-Systemen im Zusammenhang mit dem Vertrieb von Musikdownloads[127] in erster Linie auf DRM-Systeme der ersten Generation, d.h. auf Technologien, die vorwiegend auf die Einschränkung der Möglichkeit der Vervielfältigung sowie der Übertragbarkeit von digitalen Multimediawerken gerichtet sind. Solche DRM-Systeme werden nachfolgend verkürzt auch als Kopierschutztechnologien bezeichnet.[128]

B. Technischer Hintergrund

Im folgenden Abschnitt werden der Aufbau von DRM-Systemen sowie die Technologien, die hierbei typischerweise eine Rolle spielen, in Grundzügen dargestellt.[129] Grundsätzlich gibt es nicht „die eine" DRM-Technologie im Sinne einer identischen, fest gefügten technologischen Einheit. Vielmehr setzt sich jedes einzelne DRM-System aus einer Vielzahl unterschiedlicher Komponenten zusammen, die im Gesamtsystem des jeweiligen DRM-Systems eine bestimmte Funktion erfüllen.[130]

I. Grundstruktur von DRM-Systemen

Im Rahmen eines durch ein DRM-System betreuten Prozesses zur Lieferung eines digitalen Multimediawerks (im Rahmen dieses Kapitels nachfolgend als „Inhalt"

125 *Ünlü*, Content Protection, 2005, S. 47.
126 *Ünlü* s.o.
127 Vgl. 5. Kapitel, Teil A.
128 *Flechsig*, in: FS. *Nordemann*, 2004, S. 313, 317.
129 Weiterführend vgl. die sehr ausführliche Darstellung bei *Bechtold*, DRM, 2002, S. 23-101; *Fränkl/Karpf*, DRMS, 2004, S. 29-55; *Ünlü*, Content Protection, 2005, S. 60-84.
130 *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 34-35; *Arlt*, DRMS, 2006, S. 13; *ders*., GRUR 2004, S. 548, 549.

bezeichnet) an einen Nutzer lassen sich – bei allen Unterschieden zwischen verschiedenen DRM-Systemen im Detail – im Wesentlichen drei Phasen unterscheiden: die Verpackung des Inhalts zusammen mit wesentlichen, darauf bezogenen Informationen auf Ebene des „content server", die Hinzufügung von Informationen über den Umfang der erlaubten Nutzung durch den „license server" sowie die Anforderung und Lieferung des Inhalts über den Computer des Nutzers, den „client".[131]

Auf der Ebene des *content servers* wird der Inhalt durch eine Software, den „content packager", mit bestimmten Informationen[132] versehen und in einer Datei verpackt. Diese Datei wird mit Hilfe einer vom Rechtsinhaber gewählten Technologie verschlüsselt.[133] Dieses durch den *content packager* geschnürte Paket wird auf Ebene des *license server* mit Hilfe einer weitere Software, dem „DRM license generator", mit Informationen über die Nutzungsrechte versehen, die einem Nutzer an dem Inhalt seitens des Rechtsinhabers eingeräumt werden. Diesem Datenpaket wird aus einer Datenbank ein Schlüssel zugeordnet, mit dessen Hilfe die Datei wieder entschlüsselt werden kann.

Auf der Ebene des *client* sorgt eine Software, der „DRM controller",[134] dafür, dass der Computer des Nutzers mit dem *license server* bzw. dem *content server* kommunizieren kann. Der *DRM controller* ist gleichzeitig Ausgangs- und Endpunkt des Kommunikationsprozesses zwischen *content server*, *license server* und *client*. Über ihn wird dieser Kommunikationsprozess zunächst angestoßen, indem der Nutzer mit seiner Hilfe beispielsweise den Download einer bestimmten Tonaufnahme beim *content server* abfragt. Daraufhin führen *content* und *license server* die oben dargestellten Prozesse durch. Bevor jedoch der *DRM license generator* die Informationen betreffend die Nutzungsrechte und die Entschlüsselung an den *client* überträgt, verifiziert er zuvor über den *DRM controller* die Identität des Nutzers.

Weiterhin findet vor der Lieferung in der Regel ein Zahlungsvorgang statt. Dessen genauer Zeitpunkt hängt von dem einzelnen Geschäftsmodell ab, innerhalb dessen das jeweilige DRM-System eingesetzt wird. Bei einem sogenannten „direct download"-Modell findet beispielsweise die einmalige Zahlung regelmäßig vor der Lieferung des Download an den *client* statt. Im Falle eines Abonnement-Modells wird hingegen sowohl nach der ersten Registrierung des Nutzers im Voraus für die

131 Die nachfolgende Darstellung basiert im Wesentlichen auf den Ausführungen bei *Montagnani*, 26 Cardozo Arts & Ent. L.J. 719, S. 742-744; s.a. *Ünlü*, Content Protection, 2005, S. 41.

132 Wie beispielsweise die Identität des Rechtsinhabers.

133 Handelt es sich nicht um ein Download- sondern ein Streaming-Angebot, das ebenfalls mit DRMS verknüpft werden kann, so wird nur die Information über den Inhalt in der Datei verpackt und bereitgestellt, da der Inhalt selbst im Gegensatz zum Download nicht an den Nutzer ausgeliefert wird.

134 Beispielsweise die Abspielsoftware „Windows Media Player" von Microsoft.

Bereitstellung der durch das Abonnements gewährten Nutzungsmöglichkeiten für einen bestimmten Zeitraum gezahlt, sowie im Anschluss daran in regelmäßigen Intervallen abhängig von der Laufzeit des Abonnements.

II. Technologien

Nachfolgend wird die Funktionsweise von Verschlüsselungstechnologien sowie von Metadaten, Rights Expression Languages und Wasserzeichen kurz skizziert.

1. Verschlüsselungstechnologien

Diese Technologien spielen im Zusammenhang mit dem Schutz von digitalen Multimediawerken vor unberechtigtem Zugriff und vor unerlaubten Nutzungshandlungen eine wichtige Rolle. Denn durch Verschlüsselungsalgorithmen wird sichergestellt, dass nur ein Nutzer, der über eine entsprechende Berechtigung verfügt, eine Multimediawerk nutzen kann.[135] Denn ein verschlüsselter Inhalt ist ohne den entsprechenden Schlüssel für den Empfänger nutzlos.[136] Diese sogenannten „kryptographischen Technologien" stellen die am weitesten entwickelte Gruppe von DRM-Technologien dar, die daher ein relativ hohes Schutzniveau gewähren.[137]

Es ist zu unterscheiden zwischen symmetrischen, asymmetrischen und hybriden Verschlüsselungsverfahren. Im Falle eines symmetrischen Algorithmus (sogenannte „private key"-Kryptographie) verwenden sowohl der Absender als auch der Empfänger denselben Schlüssel, um die das digitale Multimediawerk enthaltende Datei zu ver- bzw. entschlüsseln.[138] Der Nachteil des symmetrischen Algorithmus besteht in der Notwendigkeit, den „private key" zusammen mit der verschlüsselten Datei an den Adressaten zu übermitteln. Denn zum einen sind mit der Generierung und Übermittlung eines eigenen Schlüssels an jeden Adressaten Kosten verbunden, und zum anderen geht mit der Übermittlung des Schlüssels ein Sicherheitsrisiko einher, da, wenn das Multimediawerk mitsamt dem Schlüssel während der Übermittlung über das Internet von einem Dritten abgefangen wird, dieser das Multimediawerk ohne weiteres decodieren und nutzen kann.[139]

135 *Ünlü*, Content Protection, 2005, S. 68.
136 *Bechtold*, DRM, 2002, S. 23.
137 *Ünlü*, Content Protection, 2005, S. 69; *Bechtold*, DRM, 2002, S. 33.
138 *Ünlü*, Content Protection, 2005, S. 69; bekannte *private-key*-Verfahren sind der Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard und International Data Encryption Standard (IDEA); *Bechtold*, DRM, 2002, S. 23 m.w.N.
139 *Bechtold*, DRM, 2002, S. 24; *Ünlü*, Content Protection, 2005, S. 69.

Hingegen kommen bei einer Technologie, die einen asymmetrischen Algorithmus verwendet (sogenannte „public key"-Kryptographie), in Bezug auf die Ver- und Entschlüsselung jeweils unterschiedliche Schlüssel zum Einsatz. Zum einen im Rahmen der Verschlüsselung ein „public key", der öffentlich bekannt und in einer Datenbank abgelegt ist, und weiterhin zur Entschlüsselung ein *private key*, der nur dem Empfänger bekannt ist und bei diesem verbleibt.[140] Das *public-key*-Verfahren ist computertechnisch komplexer – und damit langsamer – als das *private-key*-Verfahren und erfordert zudem die Errichtung einer Infrastruktur, über die der öffentlich verfügbare Schlüssel verwaltet wird.[141]

Im Rahmen des dritten, hybriden Verschlüsselungsverfahrens werden symmetrische und asymmetrische Algorithmen miteinander kombiniert.[142] Dabei wird die das Multimediawerk enthaltende Datei mit Hilfe eines symmetrischen Algorithmus verschlüsselt, der für die Codierung verwendete Schlüssel hingegen asymmetrisch codiert, bevor Datei und Schlüssel gemeinsam an den Adressaten übermittelt werden. Aufgrund der asymmetrischen Codierung des Schlüssels ist es nur dem berechtigten Empfänger möglich, diesen mit Hilfe des bei ihm deponierten *private key* zu entschlüsseln, wodurch eine Minimierung des Risikos der Übermittlung des Schlüssels zur Dekodierung der Datei über das Internet erreicht wird. Da jedoch nicht für die Datei, sondern nur für den zur Decodierung notwendigen Schlüssel, der wesentlich kleiner als die Datei ist, ein asymmetrischer Algorithmus eingesetzt wird, hält sich die computertechnische Komplexität des Übermittlungsvorgangs in Grenzen.

2. Metadaten, Rights Expression Languages und Wasserzeichen

Zum Zweck der Identifizierung und Verwaltung von Rechten durch DRM-Systeme kommen vor allem Metadaten, Rights Expression Languages und Wasserzeichen zum Einsatz.

Durch Metadaten werden „Informationen über Informationen" in standardisierter Form weitergegeben, so dass sie automatisiert verarbeitet und ausgelesen werden können.[143] Die mitgeteilten Informationen können in einer Beschreibung der charakteristischen Merkmale eines digitalisierten Inhalts, der Nutzungsbedingungen, denen ein solcher Inhalt unterliegt, oder aber in Informationen über den Nutzer bestehen, an den ein solcher Inhalt übermittelt wird.

140 *Ünlü*, Content Protection, 2005, S. 69; Beispiele für das *public-key*-Verfahren sind RSA und El Gamal; *Bechtold*, DRM, 2002, S. 24.
141 *Ünlü*, Content Protection, 2005, S. 70; *Bechtold*, DRM, 2002, S. 25.
142 *Bechtold*, DRM, 2002, S. 26.
143 *Bechtold*, DRM, 2002, S. 35 ff.

Eigens zur standardisierten Beschreibung von Nutzungsbedingungen wurden spezielle formalisierte sogenannte „rights expression languages“ („REL“) entwickelt, anhand derer diese Bedingungen in für Computer verständlicher Form einheitlich ausgedrückt werden können. [144] Mit Hilfe von REL ist es möglich, den Umfang der einem Nutzer in Bezug auf ein digitalisiertes Multimediawerk gewährten Rechte festzuhalten, wie beispielsweise Dauer und Häufigkeit der Nutzung, Qualität der Wiedergabe, die dem Nutzer erlaubten Handlungen sowie das vom Nutzer für die Vornahme einer solchen Handlung jeweils zu entrichtende Entgelt.[145] Die beiden bekanntesten REL-Standards sind die „eXtensible rights Markup Language“ (XrML) sowie die „Open Digital Rights Language“ (ODRL).[146]

Um Metadaten möglichst untrennbar mit einem digitalen Multimediawerk zu verbinden, werden Wasserzeichen-Technologien eingesetzt, die diese Informationen unmittelbar mit der digitalen Kopie des Multimediawerks verweben.[147] Eine qualitativ hochwertige Wasserzeichen-Technologie zeichnet sich dadurch aus, dass sie den jeweiligen digitalen Inhalt, dem sie Metadaten hinzufügt, nur geringfügig verändert, so dass diese Veränderung vom Nutzer nicht sinnlich wahrgenommen werden kann. Zudem darf ein Wasserzeichen nicht entfernt werden können, ohne dass der Inhalt, dem es hinzugefügt wurde, dadurch beschädigt wird.[148] Wasserzeichen-Technologien werden auch dazu eingesetzt, um digitale Multimediawerke im Internet nachzuverfolgen. Dadurch wird nachvollzogen, aus welcher Quelle ein digitales Multimediawerk ursprünglich stammt und auf welchem Weg es an den Ort gelangt ist, an dem es vom Rechtsinhaber letztlich aufgefunden wurde – beispielsweise in einem illegalen Filesharing-Netzwerk.

III. Beispiele für in der Multimediaindustrie eingesetzte DRM-Systeme

1. CDs

Mit Beginn des neuen Jahrtausends kamen in der Musikindustrie zunehmend DRM-Systeme zur Verhinderung der Auslesbarkeit von Musik-CDs über Computer zum Einsatz, um die illegale Vervielfältigung und Verbreitung von digitalen Tonaufnahmen zu verhindern.[149] Allerdings kam es seitens der Käufer solcher ko-

144 *Bechtold*, DRM, 2002, S. 46; *Ünlü*, Content Protection, 2005, S. 79.
145 *Ünlü*, Content Protection, 2005, S. 79.
146 Weiterführend vgl. *Bechtold*, DRM, 2002, S. 47 ff. (XrML), 50 ff. (ODRL).
147 *Ünlü*, Content Protection, 2005, S. 71.
148 *Bechtold*, DRM, 2002, S. 54 ff.
149 Vgl. bzgl. der Details der unterschiedlichen, konkret verwendeten Technologien den Üblick bei *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 35-37.

piergeschützter CDs bald zu massiven Beschwerden, da der Einsatz dieser Kopierschutztechnologien oftmals zu Problemen bei der Abspielbarkeit der Tonaufnahmen über ältere CD-Player führte.[150] Die bereits aus diesem Grund unter den Nutzern weit verbreitete Ablehnung[151] von Kopierschutztechnologien wurde weiterhin durch den Rootkit-Skandal[152] angeheizt. Daraufhin erklärten die Major Labels zwischen 2004 und 2007 sukzessive den Verzicht auf den Einsatz von Kopierschutztechnologien auf CDs.[153] Musik-CDs sind somit gegenwärtig wieder weitgehend frei von DRM-Systemen habbar.[154]

2. Onlineshops und Abonnementdienste

Weiterhin werden bzw. wurden DRM-Systeme im Rahmen von Internetdiensten, die digitale Tonaufnahmen als herunterladbare Dateien („Musikdownloads") über das Internet zum Kauf anbieten („Onlineshops") und zeitlich befristeten Abonnements zur Nutzung von Musik („Abonnementdienste") eingesetzt.

150 *CDT*, Evaluating DRM, 2006, S. 7; *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 36.

151 Man gebe nur die Stichworte „CD" und „kein Kopierschutz" bei Google ein, worauf man jede Menge Links zu Einträgen und Webseiten erhält, die deutliche Kritik an sowie Anleitungen und Tipps zur Umgehung von Kopierschutztechnologien zum Gegenstand haben.

152 Vgl. 5. Kapitel, Teil B.II.3.

153 Vgl. *Theurer*, Die Musikindustrie zweifelt am Kopierschutz, FAZ.NET, 04.06.2004, http://www.faz.net/s/RubE2C6E0BCC2F04DD787CDC274993E94C1/Doc~EC158B-DE6F1404D6D8A8BAD5AA28D1357~ATpl~Ecommon~Scontent.html (zuletzt abgerufen am 01.07.2010); *Heise Online*, Sony Music Japan verzichtet auf Kopierschutz, 03.10.2004, http://www.heise.de/newsticker/meldung/Sony-Music-Japan-verzichtet-auf-Kopierschutz-106635.html (zuletzt abgerufen am 01.07.2010); *gullinews*, EMI beendet die Ära kopiergeschützter CDs, 08.01.2007, http://www.gulli.com/news/emi-beendet-die-ra-kopiergesch-2007-01-08/ (zuletzt abgerufen am 01.07.2010). Allerdings war die Wirksamkeit des Einsatzes solcher Kopierschutztechnologien bereits vor diesem Schritt höchst fraglich geworden, da jede Kopierschutztechnologie innerhalb kürzester Zeit durch Hacker „geknackt" und die entsprechende Umgehungssoftware im Internet veröffentlicht worden war. Auch war der auf CDs enthaltene Kopierschutz anders als bei DVDs nicht zusätzlich mit einem entsprechenden Schutz auf den CD-Abspielgeräten kombiniert, was die Effektivität des Kopierschutzes weiter einschränkte. Vgl. hierzu *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 36.

154 Vgl. hierzu die Webseite des Bundesverbandes der Musikindustrie zum Thema Kopierschutz, http://www.musikindustrie.de/kopierschutz/ (zuletzt abgerufen am 01.07.2010); s.a. *Jobs,* Thoughts on Music, 06.02.2007, http://www.apple.com/hotnews/thoughtsonmusic/ (zuletzt abgerufen am 01.07.2010): *„In 2006, under 2 billion DRM-protected songs were sold worldwide by online stores, while over 20 billion songs were sold completely DRM-free and unprotected on CDs by the music companies themselves. The music companies sell the vast majority of their music DRM-free, and show no signs of changing this behavior, since the overwhelming majority of their revenues depend on selling CDs which must play in CD players that support no DRM system".* Dementsprechend wird auch vermutet, dass der weit überwiegende Anteil, digitaler Tonaufnahmen, die auf iPods enthalten sind, von „gerippten" CDs stammt, vgl. *Krasilovsky/Shemel*, Music Business, 2007, S. 429.

Das Geschäftsmodell, auf dem Onlineshops basieren, überträgt das tradierte, im analogen Zeitalter dominierende Vertriebsmodell der Tonträgerunternehmen ins Internet.[155] Der hauptsächliche Unterschied zum Offline-Vertrieb besteht darin, dass die Tonaufnahmen in rein digitaler Form als Datei anstatt in Form eines physischen Datenträgers erworben werden und unmittelbar auf den Computer des Nutzers heruntergeladen werden können.[156] Der iTunes-Store war der erste Onlineshop, der seinen Nutzern einen sogenannten „à la carte" oder „pay-per-download"-Service anbot, d.h. die Möglichkeit, sich eine einzelne digitale Tonaufnahme oder ein „bundle", d.h. eine Kombination mehrerer Tonaufnahmen in Form eines Albums, im Internet auszusuchen und eine digitale Kopie dieser Tonaufnahme dauerhaft zu Eigentum zu erwerben. Durch den Einsatz von DRM-Systemen wurde bis vor kurzem[157] sichergestellt, dass ein Musikdownload nur bei Vorhandensein einer bestimmten Software auf dem Computer des Nutzers und/oder nur im Zusammenhang mit der Verwendung eines vom jeweiligen Anbieter vertriebenen digitalen Endgerätes genutzt werden konnte, worüber die Einhaltung der vom Rechtsinhaber vorgegebenen Beschränkungen der Nutzbarkeit der erworbenen Dateien kontrolliert werden sollte.[158] Auch wurden nutzerseitige Handlungen in Bezug auf den Musikdownload weitgehend eingeschränkt, insbesondere die Möglichkeit der Vervielfältigung, der Bearbeitung sowie der Übertragbarkeit auf andere Computer als denjenigen, auf den die Datei ursprünglich heruntergeladen wurde.[159] Bekanntestes Beispiel für ein solches im Rahmen eines Onlineshop genutztes DRM-System ist die im Rahmen des iTunes-Store eingesetzte „Fair Play"-Technologie des Unternehmens Apple.[160]

Im Gegensatz zu Onlineshops wird im Rahmen von Abonnementdiensten nicht der dauerhafte Erwerb einzelner Tonaufnahmen oder *bundles* angeboten, sondern erhält der Nutzer gegen Zahlung einer monatlichen Gebühr einen zeitlich begrenzten Zugang zu einer Musikbibliothek, deren Inhalte er bis zum Ablauf des Abonnements jederzeit nutzen kann.[161] Der Nutzer zahlt bei diesem Modell somit nicht dafür, Eigentümer einer erlaubten Kopie einer digitalen Tonaufnahme zu werden und diese auf unbegrenzte Dauer nutzen zu können, sondern für die vorübergehend gewährte Möglichkeit der Nutzung von digitalen Tonaufnahmen. Die vom Nutzer aus der Bibliothek abgerufene Tonaufnahme wird auf den Computer des Nutzers in Form eines Live-Streams (nachfolgend „Stream" oder „Streaming-Angebot")

155 *CDT*, Evaluating DRM, 2006, S. 8; *Bernstein/Sekine/Weissman*, Global Music Industry, 2007, S. 17.
156 *Montagnani*, 26 Cardozo Arts & Ent. L.J. 719, 756 (2009).
157 Vgl. 5. Kapitel, Teil A.
158 *Perritt*, 16 Mich. St. J. Int'l Law 113, 122 (2007); *CDT*, Evaluating DRM, 2006, S. 9.
159 *CDT*, Evaluating DRM, 2006, S. 8, 9.
160 *Perritt*, 16 Mich. St. J. Int'l Law 113, 123 (2007).
161 *Montagnani*, 26 Cardozo Arts & Ent. L.J. 719, S. 757 (2009); CDT, Evaluating DRM, 2006, S. 9.

übertragen. Unter einem Stream versteht man das Empfangen und die gleichzeitige Wiedergabe von Audio- und/oder Videodateien aus einem Rechnernetz,[162] wobei die dauerhafte lokale Speicherung der Datei auf dem empfangenden Computer nicht vorgesehen ist.[163] Im Rahmen von Abonnementdiensten wird mit Hilfe von DRM-Systemen vor allem die Zugriffsberechtigung des Nutzers verifiziert. Dafür wird ein verschlüsselter Token-Code durch den Computer des Nutzers bei dem Internetdienst abgerufen, der verweigert wird, sofern keine Berechtigung seitens des jeweiligen Nutzers besteht oder sobald eine bisher bestehende Berechtigung abgelaufen ist.[164]

3. Filmbereich

Bereits im Zeitalter von Videokassetten wurden auch seitens der Filmindustrie Kopierschutztechnologien zur Verhinderung der Herstellung von Raubkopien eingesetzt. Dieser Schutz gegen die illegale Anfertigung von analogen Kopien wurde auch auf die DVD übertragen, durch die die Videokassette seit dem Jahr 1996 sukzessive ersetzt wurde, und zu diesem Zweck die Kodierungssoftware „Content Scrambling System" („CSS-Technologie") entwickelt.[165] Über diese Technologie wird der gesamte auf einer DVD gespeicherte Inhalt verschlüsselt, so dass er grundsätzlich nur von einem DVD-Player ausgelesen werden kann, der durch die „DVD Copy Control Association" lizenziert wurde und daher über die zur Entschlüsselung erforderliche Software verfügt.[166] Durch diese Verschlüsselung soll insbesondere das Auslesen von DVDs über reguläre CD-Rom-Computerlaufwerke, sowie die anschließende Recodierung des digitalen Inhalts zum Zwecke der Abspeicherung und Verbreitung des Inhaltes über CD-Rom oder über das Internet verhindert werden.[167] Für die neuste Generation an Trägermedien für Film- und Videowerke, der sogenannten „Blu-ray"-Disc,[168] wird ebenfalls ein der CSS-Kodierungssoftware vergleichbares DRM-System namens „Advanced Access Content System" eingesetzt.[169]

162 Vgl. *Wikipedia*, Stichwort „Streaming Media", Version vom 25.4.2010, 16:48 h, http://de.*Wikipedia*.org/w/index.php?title=Streaming_Media&oldid=73585843 (zuletzt abgerufen am 27.04.2010).
163 *CDT*, Evaluating DRM, 2006, S. 9-10.
164 *Perritt*, 16 Mich. St. J. Int'l Law 113, 122 (2007); *CDT*, Evaluating DRM, 2006, S. 10.
165 *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 37.
166 *CDT*, Evaluating DRM, 2006, S. 5; *Ünlü*, DRM, 2005, S. 70.
167 *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 37.
168 Die Blue-ray Disk hat sich im Februar 2008 gegen den Konkurrenten HD DVD als im Bereich *optical discs* als Nachfolgemedium der DVD durchgesetzt.
169 Vgl. *Wikipedia*, Stichwort „Advanced Acess Content System", Version vom 22.04.2010, 22:31 h, http://en.*Wikipedia*.org/w/index.php?title=Advanced_Access_Content_System&oldid=357711069 (zuletzt abgerufen am 27.04.2010).

Trotz des zweistufigen Ansatzes der CSS-Technologie, wonach bereits die DVD-Rohlinge mit dieser Software kodiert werden und weiterhin das Auslesen der DVDs an die Nutzung eines mit CSS ausgestatteten digitalen Endgeräts geknüpft ist, wurde auch dieses DRM-System zwischenzeitlich von Hackern „geknackt".[170] Dennoch stellt die CSS-Technologie, die nach wie vor beim Vertrieb von DVDs eingesetzt wird, ein relativ erfolgreiches DRM-System dar,[171] insbesondere im Vergleich mit den zahlreichen erfolglosen Versuche der Musikindustrie, einen vergleichbaren Schutz für CDs zu etablieren. Der Hauptgrund hierfür dürfte darin liegen, dass DVDs anders als CDs von Anfang an mit diesem DRM-System versehen waren und daher alle Hersteller von DVD-Abspielgeräten diese CSS-kompatibel ausstatten mussten, wodurch von Anfang an ein geschlossenes, DRM-gestütztes Schutzniveau für auf DVD veröffentlichte Filme erreicht wurde.

C. Ökonomischer Hintergrund

Vor Anbruch der Digitalisierung wurden Multimediawerke, die dem Oberbegriff der „Informationsgüter" zuzuordnen sind,[172] in der Wirtschaftstheorie als Mischgüter („impure public goods")[173] oder gar als private Güter („private goods")[174] eingeordnet, da sie aus technischen Gründen, nämlich der für den Vertrieb notwendigen Verbindung mit einem physischen Datenträger, nicht die für ein reines öffentliches Gut typischen Merkmale der Nichtrivalität („non-rivalness") und Nichtausschließbarkeit („non-excludability") aufwiesen.[175] *Non-rivalness* bedeutet, dass ein Gut von einer unbegrenzten Anzahl an Personen genutzt werden kann, ohne dass die individuelle Nutzbarkeit des Guts davon beeinträchtigt wird. Das Gut ist somit ohne Anstieg der Grenzkosten von einer Vielzahl von Personen nutzbar und damit nicht knapp („scarce").[176] Demgegenüber bedeutet *non-excludability*, dass von den Vorteilen der Nutzung des Guts niemand ausgeschlossen werden kann.[177] Da im analogen Zeitalter Multimediawerke jedoch auf physischen Datenträgern vertrieben wurden, konnten sie sich zum einen bei vielfacher Beanspruchung abnutzen. Zum anderen waren Personen, die nicht im Besitz eines solchen Datenträgers waren, von der Nutzung des Multimediaprodukts weitgehend ausgeschlossen, auch weil die illegale, d.h. außerhalb des durch die Rechtsinhaber au-

170 *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 37.
171 *Biddle/England/Peinado/Willman*, The Darknet and the Future of Content Distribution, S. 1, 11, http://msl1.mit.edu/ESD10/docs/darknet5.pdf (zuletzt abgerufen am 01.07.2010).
172 *Ünlü*, Content Protection, 2005, S. 26.
173 *Ünlü*, Content Protection, 2005, S. 36-37.
174 *Bechtold*, DRM, 2002, S. 285.
175 *Ünlü*, Content Protection, 2005, S. 37.
176 *Bechtold*, DRM, 2002, S. 284; *Ünlü*, Content Protection, 2005, S. 36.
177 *Bechtold*, DRM, 2002, S. 284-285; *Ünlü*, Content Protection, 2005, S. 36.

torisierten Produktionsablaufes stattfindende Vervielfältigung von physischen Datenträgern technisch aufwendig und kostenintensiv war.[178] Analoge Multimediaprodukte waren somit *rivalrous* und *excludable*, und bereits aufgrund dieser Merkmale in ihrer natürlichen Beschaffenheit vor unautorisierter Nutzung in gewissem Maße gefeit.[179]

Diese natürliche Beschaffenheit multimedialer Güter hat sich mit der Möglichkeit, diese zu digitalisieren, grundlegend geändert.[180] In Dateiform umgewandelte Multimediawerke können auf einer Vielzahl digitaler Endgeräte mit entsprechendem Speicherplatz abgespeichert sowie mit geringem Aufwand und ohne jeglichen Qualitätsverlust vervielfältigt werden. Verfügt der jeweilige Nutzer zudem über einen Internetanschluss, können digitale Kopien des Multimediawerks über das Internet an beliebige Orte übermittelt und dort von den Empfänger abgespeichert sowie weiter vervielfältigt und verbreitet werden.[181] Die Verbindung des multimedialen Inhalts mit einem bestimmten physischen Datenträger, die in der analogen Welt notwendige Voraussetzung für den Vertrieb und die Nutzung eines Multimediawerks war, wird damit obsolet. Das einzig verbleibende notwendige Trägermedium ist der austauschbare Speicherplatz auf digitalen Endgeräten. Dessen Fassungsvermögen wächst aufgrund des technischen Fortschritts ständig.[182]

Diese Entwicklung hat zur Folge, dass digitale Multimediawerke nunmehr uneingeschränkt die Merkmale der *non-excludability* und *non-rivalness* öffentlicher Güter erfüllen.[183] Denn die digitale Kopie kann sich auch durch wiederholtes Abrufen nicht abnutzen und zudem unbegrenzt vervielfältigt werden.[184] Zudem bedeutet die gleichzeitige Verfügbarkeit effizienter und preiswerter Vervielfältigungs- und Datenkomprimierungstechnologien sowie schneller breitbandiger Internetanschlüsse, einschließlich der damit einhergehenden Datennetzwerke und Software zum Suchen und Tausch bestimmter Dateien, dass digitale Multimediawerke schnell, einfach und billig weltweit verbreitet werden können. Es ist daher kaum mehr möglich, einen Nutzer vom Konsum eines einmal in digitaler Form

178 *Ünlü*, Content Protection, 2005, S. 37.
179 *Ünlü*, Content Protection, 2005, S. 40.
180 Genauer gesagt steht der Begriff „Digitalisierung" für eine technische Form der Datenaufzeichnung und –übermittlung, bei der die betreffenden Daten in einen Binärcode, d.h. in eine Abfolge von Zahlen, konvertiert werden, der zum Zwecke der sensorischen Aufnahme des Menschen auf einem Personal Computer oder einem anderen Endgerät wieder in analoge Form ungewandelt wird, vgl. *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007, S. 18; *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, 2006, S. 10-12.
181 *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, S. 12.
182 *Ünlü*, Content Protection, 2005, S. 41; *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, S. 12; *Grimm*, in: *Roßnagel*, Digitale Rechteverwaltung, 2009, S. 27; *Krasilovsky/ Shemel*, Music Business, 2007, S. 419.
183 *Cooter/Ulen*, Law & Economics, 2008, S. 45.
184 *Ünlü*, Content Protection, 2005, S. 41 m.V.a. den Kryptographie-Experten Bruce Schneier und dessen Ausspruch „Digital files cannot be made uncopyable, any more than water can be made not wet".

vorliegenden Multimediawerks effektiv auszuschließen.[185] Im Zeitalter der Digitalisierung werden Multimediawerke somit zu idealen öffentlichen Gütern.

Nach der Wirtschaftstheorie ist jedoch davon auszugehen, dass im Falle von öffentlichen Gütern der Markt nicht zu optimalen Ergebnissen führen wird. Denn aufgrund des sogenannten „Trittbrettfahrer-Problems" („free riding") ist auf einem solchen Markt von einem baldigen Marktversagen auszugehen.[186] Denn die *non-rivalness* und *non-excludability* des öffentlichen Guts führt dazu, dass jeder in den Besitz dieses Guts kommen, es vervielfältigen und diese Vervielfältigungsstücke in Konkurrenz zum ursprünglichen Anbieter des Guts auf dem Markt anbieten kann. Da jedoch einem Anbieter, der lediglich ein bereits vorhandenes, digitalisiertes Gut kopiert (nachfolgend „free rider"), für diese Vervielfältigung wesentlich geringere Kosten anfallen als dem ursprünglichen Hersteller für die Produktion dieses Guts kann der *free rider* das Gut zu einem billigeren Preis auf dem Markt anbieten als der Hersteller. Dies führt zu einem Preisverfall, aufgrund dessen es dem Hersteller langfristig nicht mehr möglich ist, die von ihm in die Produktion des Guts investierten Kosten über dessen Vertrieb zu amortisieren. Damit entfällt jedoch der wirtschaftliche Anreiz zur Investition in die Produktion des Guts. Im Ergebnis wird der Markt somit nicht mehr ausreichende Mengen des öffentlichen Guts produzieren, da niemand dazu bereit sein wird, in dessen Produktion zu investieren, da er den anschließenden Vertrieb, d.h. die Vervielfältigung und Verbreitung des Guts, nicht kontrollieren, d.h. den wirtschaftlichen Erfolg seiner Investition nicht absichern kann.[187]

Die Multimediaindustrie sieht sich somit vor der Herausforderung, Wege zu finden, um ein solches Marktversagen beim Vertrieb von Multimediawerken zu verhindern. Es gilt sicherzustellen, dass sich Investitionen in die Herstellung von Multimediawerken trotz des Trittbrettfahrerproblems weiterhin lohnen.[188] Ein Ansatz zur Lösung des Trittbrettfahrerproblems ist die Einräumung einer Rechtsposition an dem öffentlichen Gut (sogenannte „rechtliche Lösung").[189] Denn hierdurch wird das Merkmal der *non-excludability* eliminiert, indem der Hersteller des Guts Dritte von dessen unautorisierten Nutzung auf rechtlichem Wege auszuschließen vermag. An Multimediawerken bestehen jedoch bereits urheberrechtliche Rechtspositionen, vor allem in Form der in Bezug auf ein urheberrechtlich geschütztes Werk eingeräumten Verwertungsrechte.[190] Diese Rechtspositionen

185 *Ünlü* s.o.
186 *Schäfer/Ott*, Economic Analysis of Law, 2004, S. 93.; *Cooter/Ulen*, Law & Economics, 2008, S. 46; *Bechtold*, DRM, 2002, 286 f..
187 *Ünlü*, Content Protection, 2005, S. 42.
188 *Ünlü*, Content Protection, 2005, S. 43.
189 *Bechtold*, DRM, 2002, S. 287 f.; *Ünlü*, Content Protection, 2005, S. 42; vgl. zu den verschiedenen theoretischen Ansätzen einer rechtlichen Lösung *Schäfer/Ott*, Economic Analysis of Law, 2004, S. 96 ff.
190 Vgl. 5. Kapitel, B.III.1.

entfalten jedoch angesichts der praktischen Schwierigkeiten, Nutzungs-, Vervielfältigungs- und Verbreitungsrechten in Bezug auf ein digitales Multimediawerk gegenüber einzelnen Nutzern durchzusetzen, derzeit nur eine eingeschränkte Wirkung.[191]

An dieser Stelle kommen nunmehr DRM-Systeme ins Spiel. Denn wenn es mit ihrer Hilfe gelänge, die tatsächliche Durchsetzbarkeit der den Rechtsinhabern gewährten Rechte in Bezug auf die Nutzung, Vervielfältigung und Verbreitung von digitalen Multimediawerken auf technischem Wege sicherzustellen, würde dadurch die *excludability* dieser Güter wiederhergestellt und damit dem Trittbrettfahrerproblem die Grundlage entzogen.[192] Dann ließen sich die tradierten Geschäftsmodelle der analogen Welt auf den Vertrieb von Multimediawerken in digitaler Form übertragen.[193] Aus ökonomischer Sicht könnten somit DRM-Systeme zur rechtlichen Lösung des Problems drohenden Marktversagens durch Trittbrettfahrer beitragen oder sogar das Problem als Alternative[194] zum rechtlichen Lösungsansatz auf rein technischem Wege lösen.

D. Rechtlicher Hintergrund

Aus ökonomischer Perspektive verbindet sich mit DRM-Systemen die Hoffnung, das tradierte Geschäftsmodell der Multimediaindustrie zu bewahren und ein Marktversagen als Ergebnis der Digitalisierung zu verhindern.[195] Daher wurden zum Schutz von Systemen, die beim Vertrieb von digitalen Multimediawerken zum Zwecke des Schutzes von Urheberrechten eingesetzt werden („technische Schutzmaßnahmen"), zunächst auf internationaler und wenig später auch auf nationaler Ebene in den USA, der EU und Deutschland spezielle Vertrags- bzw. Gesetzeswerke erlassen.[196]

Diese Rechtssetzungsakte basierten auf der Überzeugung, dass technische Schutzmaßnahmen ohne eine Absicherung durch einen speziellen gesetzlichen

191 *Ünlü*, Content Protection, 2005, S. 42.
192 *Akester*, Technological Accomodation, 2009, S. 11; *Samuelson/Schultz*, 6 J. Telecom. & High Tech. L. 41, 42 (2007).
193 *Frahm*, Zukunft der Tonträgerindustrie, 2007, S. 84.
194 *Bechtold*, DRM, 2002, S. 289.
195 *Vinje*, EIPR 1996, 431.
196 Vgl. hierzu beispielsweise das *Grünbuch der Europäischen Kommission zum Urheberrecht und zu den verwandten Schutzrechten in der Informationsgesellschaft*, worin ausgeführt wird, dass die Digitalisierung *„die Identifizierung, die Kennzeichnung, den Schutz und die automatische Verwaltung"* von urheberrechtlich geschützten Werken erlaube und es erforderlich *„scheint, dass solche Systeme geschaffen und international durchgesetzt werden"*, um zu vermeiden, dass *„die Informationsgesellschaft den Rechtsinhabern zum Nachteil gereicht"*, KOM(95) 382 endg., S. 79; *Ficsor*, WIPO Treaties, 2002, Chapter 7, Art. 11, Rn. C11.01.

Schutz alsbald von den Nutzern umgangen werden würden und somit ein „arms race“ zwischen immer neuen technischen Schutzmaßnahmen auf Seiten der Rechtsinhaber einerseits und Technologien zur ihrer Umgehung auf Seiten der Nutzer andererseits die unvermeidliche Folge wäre.[197] Weiterhin verfolgen die Regelungen den Zweck, eine durch Technologien ermöglichte, individualisierte Abwicklung von Lizenzverträgen über das Internet zu unterstützen.[198]

I. Die 1996’er WIPO-Internetverträge

Die sogenannten „WIPO-Internetverträge“, d.h. der WIPO-Urheberrechtsvertrag („WIPO Copyright Treaty“, „WCT“)[199] und der WIPO-Vertrag über Darbietungen und Tonträger („WIPO Performances and Phonograms Treaty“, „WPPT“),[200] vom 20. Dezember 1996 waren das Ergebnis der im Dezember 1996 in Genf tagenden „Diplomatic Conference on Certain Copyright and Neighboring Rights Questions“, an der Vertreter von etwa 150 Staaten teilnahmen,[201] darunter die 127 Mitgliedstaaten der World Intellectual Property Organisation („WIPO“) sowie die Europäische Gemeinschaft.[202]

Der WCT ist ein Sonderabkommen im Sinne von Art. 20 der Revidierten Berner Übereinkunft („RBÜ“),[203] dessen Regelungen die Geltung des RBÜ nicht berühren[204] und dessen Vertragsparteien nicht notwendigerweise auch Partei des RBÜ sein müssen.[205] Er trat am 6. März 2002 in Kraft und wurde bisher von 88 Staaten ratifiziert.[206] Der WPPT stellt hingegen ein vom RBÜ unabhängiges, eigenständiges Vertragswerk dar, das am 20. Mai 2002 in Kraft trat und bisher von 86 Staaten ratifiziert wurde.[207] Die USA traten den WIPO-Internetverträgen bereits zum Zeitpunkt des Inkrafttretens der Verträge am 6. März bzw. 20. Mai 2002 bei. Der Bei-

197 *Spindler*, GRUR 2002, S. 105, 115; *Arlt*, DRMS, 2006, S. 59, 60; krit. *Vinje*, EIPR 1996, 431, 439.
198 *Reinbothe/von Lewinski*, WIPO Treaties, 2002, Art. 11 WCT, Rn. 12.
199 S. Treaty Doc. No. 105-17, S. 1 (1997)/ 36 I.L.M. 65; deutsche Fassung veröffentlicht in ABlEG 1998 Nr. C. 165, S. 9.
200 S. Treaty Doc. No. 105-17, S. 18 (1997)/36 I.L.M. 76; deutsche Fassung veröffentlicht in ABlEG 1998, Nr. C 165, S. 13.
201 *Nimmer,* in: Nimmer on Copyright, 2009, § 12A.01[B], S. 12A-8.
202 *Wand*, Technische Schutzmaßnahmen, 2001, S. 230. Für einen Überblick über Entstehungsgeschichte und Inhalt der Vertragswerke vgl. *von Lewinski/Gaster*, ZUM 1997, 607 ff.; s.a. *Hoeren*, MMR 2000, 515 ff.
203 Revidierte Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst vom 9. September 1886, zuletzt geändert am 28. September 1979.
204 Vgl. Art. 1 WCT.
205 Vgl. Art. 17 WCT.
206 Stand 28.08.2008. Der jeweils aktuelle Stand ist abrufbar unter http://www.wipo.int/treaties/en/ip/wct/.
207 Stand 28.08.2008. Der jeweils aktuelle Stand ist abrufbar unter http://www.wipo.int/treaties/en/ip/wppt/.

tritt der EU und deren Mitgliedstaaten einschließlich Deutschland wurde hingegen erst zum 14. März 2010 wirksam.

In Art. 11 WCT, Art. 18 WPPT adressieren die WIPO-Internetverträge das Problem der Umgehung technischer Schutzmaßnahmen, indem die Vertragsstaaten verpflichtet werden, „adäquaten Rechtsschutz und wirksame Rechtsmittel zur Verfügung zu stellen gegen die Umgehung wirksamer technologischer Maßnahmen, die von Urhebern in Verbindung mit den ihnen unter diesem Vertrag oder dem RBÜ gewährten Rechten eingesetzt werden und die solche, auf ihre Werke bezogenen Handlungen unterbinden, die nicht von den betroffenen Urhebern genehmigt bzw. gesetzlich erlaubt sind".[208] Im einzelnen waren die notwendigen Voraussetzungen eines solchen Umgehungsverbots unter den Konferenzteilnehmern umstritten, weswegen die endgültige Formulierung dieser Verpflichtung recht allgemein ausfiel und damit den Vertragsstaaten in Bezug auf die Details einer solchen Regelung ein erhebliches Maß an Gestaltungsspielraum bei der Umsetzung dieser Vorgabe eingeräumt wurde.[209]

Weiterhin werden die Vertragsstaaten in Art. 12 WCT, Art. 19 WPPT verpflichtet, adäquate und wirksame Rechtsmittel zur Verfügung zu stellen, zum einen gegen die unbefugte Entfernung oder Verfälschung elektronischer Informationen betreffend die Verwaltung von Urheberrechten („copyright management information") und zum anderen gegen die Verbreitung von Kopien von Werken ohne bzw. mit verfälschter *copyright management information*. Hierdurch sollte auch der Beeinträchtigung von Informationssystemen, die zu der Durchsetzung von Rechtspositionen beitragen und aus diesem Grund als schutzwürdig angesehen wurden, entgegengewirkt werden,[210] um damit den Rechtsinhabern die Feststellung der unberechtigten Nutzung bzw. den Nachweis der Rechtsinhaberschaft an urheberrechtlich geschützten Werken zu erleichtern.[211] Die Voraussetzungen dieses Verbotstatbestandes wurden detaillierter ausgestaltet als diejenigen des Umgehungsverbots technischer Schutzmaßnahmen. Insbesondere wurden zivilrechtliche Rechtsbehelfe an das Vorliegen von Kenntnis seitens des Verletzers von der Unrichtigkeit der in Frage stehenden *copyright management information* geknüpft.[212]

Die in Art. 11, 12 WCT bzw. Art. 18, 19 WPPT niedergelegten Verpflichtungen unterscheiden sich maßgeblich von den sonstigen in den WIPO-Internetverträgen

208 *von Lewinski/Gaster*, ZUM 1997, 607, 618-619.
209 *von Lewinski/Gaster*, ZUM 1997, 607, 619.
210 *von Lewinski/Gaster*, s.o.; *Wand*, Technische Schutzmaßnahmen, 2001, S. 47; *Reinbothe/von Lewinski*, WIPO Treaties, 2002, Art. 12 WCT, Rn. 9; *Czychowski*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 95 c Rn. 4.
211 *Wand*, Technische Schutzmaßnahmen, 2001, S. 8; ebenso *Arlt*, DRMS, 2006, S. 145; *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, S. 95; *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010 § 35 Rn. 2.
212 *von Lewinski/Gaster*, ZUM 1997, 607, 619.

getroffenen Vereinbarungen, indem sie konkrete neue Regelungen enthalten, die das bereits bestehende internationale Recht ergänzen und nicht nur bereits bestehende Regelungen interpretieren oder modifizieren.[213] Sie stellen daher das Kernstück der WIPO-Internetverträge dar.[214]

II. Die Umsetzung der WIPO-Internetverträge in den USA, der EU und Deutschland

Nachfolgend wird die Umsetzung der Vorgaben aus den WIPO-Internetverträgen in das US-amerikanische und deutsch-europäische Recht dargestellt.

1. USA: Digital Millennium Copyright Act

In den USA wurden die WIPO-Internetverträge durch den I. Titel des am 28. Oktober 1998 in Kraft getretenen Digital Millennium Copyright Act („DMCA")[215] in US-amerikanisches Recht umgesetzt.[216] Hierdurch wurden mit 17 U.S.C. § 1201 ausführliche Regelungen betreffend das Verbot der Umgehung technischer Schutzmaßnahmen sowie in 17 U.S.C. § 1202 das Verbot der Fälschung und Veränderung von *copyright management information* in den *Copyright Act* eingeführt.

a. 17 U.S.C. § 1201: Das Verbot der Umgehung technischer Schutzmaßnahmen

17 U.S.C. § 1201 sanktioniert zum einen diejenigen, die unberechtigterweise eine technische Schutzmaßnahme umgehen.[217] Darüber hinaus richtet sich die Regelung aber auch gegen Personen, die eine technische Schutzmaßnahme nicht selbst umgehen, sondern lediglich die Mittel hierfür zur Verfügung stellen (sogenannte „Vorfeldmaßnahmen"). Es werden somit nicht nur Verhaltensweisen sanktioniert, die unmittelbar zu einer Urheberrechtsverletzung führen, sondern darüber hinaus

213 *Ficsor*, WIPO Treaties, Chapter 7, Art. 11, Rn. C11.01.
214 *Freytag*, MMR 1999, 207; *Czychowski*, NJW 2003, 2409, 2410; *Reinbothe*, ZUM 2002, 43, 47.
215 Pub. L. No. 105-304, 112 Stat. 2860 (28.10.1998).
216 Vgl. weiterführend zu den Regelungen des DMCA allgemein *Nimmer*, in: Nimmer on Copyright, 2009, §§ 12A und 12B; *Goldstein*, Copyright, § 5.16 ff., S. 5:241 ff; *Samuelson*, 14 Berkeley Tech. L. J. 519 (1999); *Ginsburg*, 23 Colum.-VLA J. L. & Arts 137 ff. (1999); in der deutschen Literatur vgl. beispielsweise *Freytag*, MMR 1999, 207 ff.; *Wand*, Technische Schutzmaßnahmen, 2001, S. 218 ff.
217 *Nimmer*, in: Nimmer on Copyright, 2009, § 12A.03[A], 12A-15.

auch die Herstellung von Produkten, die diese Verhaltensweisen befördern oder erst ermöglichen.[218]

Bezüglich der Anwendbarkeit von 17 U.S.C. § 1201 ist zwischen technischen Schutzmaßnahmen zu unterscheiden, die den unbefugten *Zugang* zu Werken unterbinden, und sonstigen technischen Maßnahmen, die die unbefugte Ausübung der unter dem *Copyright Act* ausschließlich dem Urheber gewährten Rechte verhindern.[219] 17 U.S.C. § 1201 erfasst nur die Umgehung ersterer Gruppe, d.h. solcher technischen Schutzmaßnahmen, die den unberechtigten *Zugang* zu einem Werk verhindern.[220] Ziel der Vorschrift ist somit zu verhindern, dass eine Person, die durch eine technische Schutzmaßnahme von dem Zugang zu einem Multimediawerk ausgeschlossen wird, widerrechtlich in den durch die technische Schutzmaßnahme geschaffenen Schutzraum, in dem sich das Multimediawerk befindet, einbricht.[221] Daher ist der Verbotstatbestand nicht erfüllt, wenn die technische Schutzmaßnahme, die der Nutzer umgeht, „nur" dazu eingesetzt wird, unerlaubte, dem Rechtsinhaber vorbehaltene Verwertungshandlungen zu unterbinden. Denn gegen solche Handlungen wird der Rechtsinhaber bereits durch die allgemeinen Regelungen des *Copyright Act* gemäß 17 U.S.C. §§ 106, 501 geschützt. Es spielt daher für die Erfüllung des Verbotstatbestands gem. 17 U.S.C. § 1201 keine Rolle, ob die von einem Nutzer vorgenommene Handlung über die Umgehung der technischen Schutzmaßnahme hinaus auch zu einer Verletzung eines der dem Rechtsinhaber ausschließlich zugewiesenen Verwertungsrechte führt.[222]

Die technische Schutzmaßnahme muss zum Schutz eines Werks eingesetzt werden, das nach US-amerikanischem *copyright law* schutzfähig ist.[223] Dies bedeutet, dass die Umgehung einer technischen Schutzmaßnahme, die ein gemeinfreies Werk schützt, nicht den Verbotstatbestand von 17 U.S.C. § 1201 erfüllt. Weiterhin muss die technische Schutzmaßnahme technisch in der Lage sein, den Zugang zu dem Werk „effektiv zu kontrollieren". Mit der Maßnahme muss somit bei ordnungsgemäßem Einsatz regelmäßig sichergestellt werden können, dass dem Nutzer Zugang zu dem Werk nur gewährt wird nach Beibringung bestimmter Informatio-

218 *Nimmer*, s.o.
219 *Goldstein*, Copyright, § 5.17, S. 5:244.
220 *Freytag*, MMR 1999, 207, 208.
221 *Nimmer*, in: Nimmer on Copyright, 2009, § 12A.03[A][1][a], 12A-16.
222 *Goldstein*, Copyright, § 5.17, S. 5:244.
223 *Nimmer*, in: Nimmer on Copyright, 2009, § 12A.03[A][1][a], 12A-16.

nen bzw. nach der Durchführung eines bestimmten Verfahrens, aus dem hervorgeht, dass der Rechtsinhaber in die Gewährung des Zugangs eingewilligt hat.[224]

Über den unmittelbaren Akt der Umgehungshandlung hinaus sind im Rahmen von 17 U.S.C. § 1201 auch darauf gerichtete Vorfeldmaßnahmen verboten, d.h. bereits die Herstellung und der Vertrieb von Werkzeugen und Geräten, die primär dem Zweck der Umgehung von technischen Schutzmaßnahmen dienen.[225] Hierunter fallen – anders als im Zusammenhang mit dem unmittelbar gegen die Umgehungshandlung gerichteten Verbot – auch Werkzeuge und Geräte, die bei der Umgehung einer technischen Schutzmaßnahme behilflich sind, die nicht den unerlaubten *Zugang* zu einem digitalen Multimediawerk, sondern die unerlaubte Ausübung eines der dem Rechtsinhaber ausschließlich vorbehaltenen Verwertungsrechte verhindern sollen.[226] Mit der Sanktionierung solcher Vorfeldmaßnahmen geht der DMCA über die Vorgaben der WIPO-Internetverträge hinaus.[227]

Die Regelungen in 17 U.S.C. § 1201(d)-(g) enthalten weiterhin zahlreiche Ausnahmen von dem Umgehungsverbot, beispielsweise zugunsten von Bibliotheken und anderen Bildungseinrichtungen, sowie zum Zwecke des „reverse engineering" und „encryption research", d.h. der Rekonstruktion und Decodierung von technischen Schutzmaßnahmen vor allem zu Forschungszwecken.

b. 17 U.S.C. § 1202: Schutz von copyright management information

17 U.S.C. § 1202 verbietet es, falsche *copyright management information* zu verwenden oder zu vertreiben, um hierdurch Urheberrechtsverletzungen zu ermöglichen, zu erleichtern oder zu verdecken. In subjektiver Hinsicht stellt der Tatbestand eine zweifache Anforderung.[228] Zum einen müssen die Tatbestandshandlungen der Verwendung bzw. des Vertriebes wissentlich vorgenommen werden. Zum anderen

224 Vgl. 17 U.S.C. § 1201(a)(3)(B): *„...a technological measure ‚effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work"*. In den Gesetzgebungsmaterialien, H.R. Rep. 105-551 (II), S. 39 heißt es hierzu weiter: *„In the Committee's view, measures that can be deemed to `effectively control access to a work' would be those based on encryption, scrambling, authentication, or some other measure which requires the use of a `key' provided by a copyright owner to gain access to a work."*

225 *Nimmer*, in: Nimmer on Copyright, 2009, § 12A.03[B], 12A-30.7, 12A-31.

226 Vgl. 17 U.S.C. § 12011(b)(1): *"... is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects* a right *of a copyright owner ... in a work or a portion thereof"* (Hervorhebung durch die Verfasserin); *Nimmer* in: Nimmer on Copyright, 2009, § 12A.03[C], 12A-32 - 12A-34.

227 *Freytag*, MMR 1999, 207, 208.

228 *Nimmer*, in: Nimmer on Copyright, 2009, § 12A.10[A][1], 12A-128 f.

muss der Verletzer mit der Absicht gehandelt haben, durch die tatbestandliche Handlung eine Urheberrechtsverletzung zu fördern.

Weiterhin sanktioniert die Vorschrift auch die Änderung oder Entfernung von *copyright management information* ohne Erlaubnis des Rechtsinhabers, den Vertrieb von Kopien von Werken, die manipulierte *copyright management information* enthalten sowie den Vertrieb von manipulierter *copyright management information* selbst. Dabei ist jeweils erforderlich, dass der Handelnde weiß oder – sofern der Verstoß gegen 17 U.S.C. § 1202 im Zusammenhang mit zivilrechtlichen Rechtsbehelfen gerügt wird – zumindest hätte wissen müssen, dass durch seine Handlung Urheberrechtsverletzungen ermöglicht, erleichtert oder verdeckt werden. Im Gegensatz zum Umgehungsverbot von technischen Schutzmaßnahmen werden von 17 U.S.C. § 1202 keine Vorfeldmaßnahmen in Bezug auf die Manipulation von *copyright management information* erfasst.[229]

Der Begriff der *copyright management information* wird in 17 U.S.C. § 1202(c) definiert als Informationen, die im Zusammenhang mit Kopien, Tonaufnahmen, Abbildungen oder Aufführungen eines Werks, gegebenenfalls auch in digitaler Form, übermittelt werden. Die Informationen müssen einer der in der Vorschrift enumerativ aufgeführten acht Kategorien zugeordnet werden können, wie z.B. Informationen, die der Identifikation des Werks, des Autors oder des ein Werk aufführenden ausübenden Künstlers dienen.[230] Auch Informationen über die Nutzungsbedingungen, denen ein Werk unterliegt, sind als *copyright management information* zu qualifizieren. Ausdrücklich von der Legaldefinition ausgeschlossen sind hingegen personenbezogene Informationen über den Nutzer eines Werks.[231]

c. Rechtsfolgen

Im Falle eines Verstoßes gegen eines der vorgenannten Verbote ist der Rechtsinhaber gemäß 17 U.S.C. § 1203 berechtigt, Klage bei einem Bundesgericht zu erheben, gerichtet entweder auf die Zahlung von Schadensersatz oder auf Erlass einer dauerhaften Handlungs- oder Unterlassungsverfügung. Der Geschädigte hat die

229 *Nimmer*, in: Nimmer on Copyright, 2009, § 12A.08, 12A-113.

230 Vgl. hierzu ausführlich *Nimmer*, in: Nimmer on Copyright, 2009, § 12A.09[A][1], 12A-117 ff.

231 Vgl. H.R. Rep. 105-551 (I), S. 22: *"It also should be noted that the definition of ‚copyright management information' does not encompass, nor is it intended to encompass, tracking or usage information relating to the identity of users of the works. The definition of [copyright management information] encompasses only the types of information listed, such as the author's name, the copyright owner's name, copyright notice information, and title of the work. It would be inconsistent with the purpose and construction of this bill and contrary to the protection of privacy to include tracking and usage information within the definition of [copyright management information]."*.

Wahl, entweder den tatsächlich erlittenen Schaden vom Verletzer ersetzt zu verlangen oder aber den pauschalierten Schadensersatz gemäß 17 U.S.C. § 1203(c)(3) zu fordern.[232] Weiterhin sieht 17 U.S.C. § 1204 als strafrechtliche Sanktion eine Geldstrafe von bis zu US$ 500.000 bzw. eine Freiheitsstrafe von bis zu fünf Jahren bei Erstbegehung vor, wenn einer der Verbotstatbestände vorsätzlich und in der Absicht verwirklicht wird, hierdurch einen wirtschaftlichen Vorteil zu erlangen.

2. EU und Deutschland: Multimediarichtlinie und Erster Korb der Urheberrechtsreform

Auf EU-Ebene wurden die Verpflichtungen aus den WIPO-Internetverträgen betreffend technische Schutzmaßnahmen und *copyright management information* durch die Richtlinie 2001/29/EG („Multimediarichtlinie")[233] umgesetzt.[234] Deren Vorgaben wurden wiederum vom deutschen Gesetzgeber durch den „Ersten Korb" der Reform des Urheberrechts in Form des Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft vom 16. August 2002[235] in das deutsche Recht eingefügt.[236]

232 Vgl. hierzu *Nimmer*, in: Nimmer on Copyright, 2009, § 12A.13, 12A-159 ff.

233 Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22.05.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABlEG Nr. L 167 vom 22.6.2001, S. 10-19. Im Jahr 2007 veröffentlichte die *Europäische Kommission* einen Bericht betreffend die Umsetzung und Auslegung durch die Mitgliedstaaten von u.a. Art. 6 der Richtlinie, vgl. den Bericht über die Anwendung der Richtlinie über die Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (2001/29/EG), abrufbar unter http://ec.Europa.eu/internal_market/copyright/copyright-infso/copyright-infso_en.htm.

234 Vgl. hierzu *Bayreuther*, ZUM 2001, 829 ff; *Hoeren*, MMR 2000, 515 ff.; *Kröger*, CR 2001, 316 ff; *Spindler*, GRUR 2002, 105 ff.

235 BGBl I S. 1774 ff.; das Gesetz trat am 13.9.2003 in Kraft. Mit dem Ersten Korb wurden zunächst die zwingenden Vorgaben der Multimediarichtlinie, die gemäß Art. 13 bis spätestens zum 22.12.2002 umgesetzt werden mußten, in deutsches Recht überführt; die Umsetzung der Kann-Vorschriften der Multimediarichtline erfolgte vier Jahre später mit dem „Zweiten Korb", d.h. durch das Zweite Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft vom 26.10.2007, BGBl I 2007 S. 2513 ff.; vgl. *Schippan*, ZUM 2003, 378.

236 Vgl. zum Ersten Korb allgemein *Czychowski*, NJW 2003, 2409 ff.; *Dreier*, ZUM 2002, 28 ff.; *Lauber/Schwipps*, GRUR 2004, 293 ff.; *Lehmann*, CR 2003, 553 ff.; *Reinbothe*, ZUM 2002, 43 ff.; *Schippan*, ZUM 2003, 378 ff.; *ders*., ZUM 2003, 678 ff. Zur Verfassungsmäßigkeit von technischen Schutzmaßnahmen vgl. *Holznagel/Brüggemann*, MMR 2003, 767 ff.

a. Das Verbot der Umgehung technischer Schutzmaßnahmen gem. Art. 6 Multimediarichtlinie bzw. § 95 a UrhG

aa. Überblick über den Regelungsgehalt

Gemäß Art. 6 Abs. 1 Multimediarichtlinie müssen die Mitgliedsstaaten für „angemessenen Rechtsschutz" gegen die vorsätzliche oder fahrlässige Umgehung einer wirksamen technischen Schutzmaßnahme sorgen. § 95 a Abs. 1 UrhG verbietet daher die Umgehung einer zum Schutz eines urheberrechtlichen Werks eingesetzten „wirksamen technischen Maßnahme".[237]

„Technische Maßnahmen" sind gemäß § 95 a Abs. 2 UrhG „Vorrichtungen und Bestandteile, die im normalen Betrieb dazu bestimmt sind, geschützte Werke oder andere nach diesem Gesetz geschützte Schutzgegenstände betreffende Handlungen, die vom Rechtsinhaber nicht genehmigt sind, zu verhindern oder einzuschränken". Damit ist der deutsche Gesetzgeber der in Art. 6 Abs. 3 Multimediarichtlinie vorgegebenen Definition weitgehend gefolgt,[238] wonach hierunter „jede Technologie, Vorrichtung oder Bestandteil, die im normalen Betrieb die von den Rechtsinhabern nicht genehmigte Handlungen verhindern oder einschränken soll" zu verstehen ist. Hierunter fallen sämtliche mögliche Komponenten eines DRM-Systems, d.h. software- ebenso wie hardwarebasierte Mechanismen der Zugangskontrolle, der Verschlüsselung, des Kopierschutzes etc.[239] Es genießen jedoch nur in Bezug auf ein Werk oder einen anderen urheberrechtlichen Schutzgegenstand eingesetzte technische Schutzmaßnahmen Rechtsschutz.[240] Nicht in den Schutzbereich von § 95 a UrhG fallen somit Schutzmaßnahmen, die die Nutzung gemeinfreier Werke kontrollieren.[241] Weiterhin müssen die technischen Schutzmaßnahmen „im normalen Betrieb" dazu bestimmt sein, Handlungen in Bezug auf einen schutzfähigen Gegenstand zu verhindern. Dies bedeutet, dass die Schutzfunktion nicht lediglich

237 In Form des auf Art. 4 der Zugangskontrollrichtlinie (Richtlinie 1998/84/EG des Europäischen Parlaments und des Rates über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten vom 20.11.1998, ABlEG L 320, S. 54 ff.) basierenden Zugangskontrolldiensteschutzgesetz (ZKDSG) existiert ein weiteres Gesetz, das die Umgehung technischer Schutzmaßnahmen sanktioniert. Der Schutz dieses Gesetz richtet sich allerdings auf technische Maßnahmen, die den Schutz des Zugangs zu zugangskontrollierten Rundfunkdarbietungen, Tele- und Mediendiensten bezwecken. Da im Zusammenhang mit dieser Arbeit jedoch nur der durch §§ 95 a UrhG gewährte Umgehungsschutz von technischen Maßnahmen interessiert, die unmittelbar den Zugang zu und die Nutzung eines urheberrechtlich geschützten Werkes schützen, wird auf das ZKDSG nicht weiter eingegangen; vgl. weiterführend zum ZKDSG beispielsweise *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, S. 57 ff.; *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 33 Rn. 26 ff.

238 *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 34 Rn. 1.

239 *Blocher*, in: *Roßnagel*, Digitale Rechteverwaltung, 2009, S. 43.

240 *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 34 Rn. 2.

241 *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 95 a Rn. 14.

das Ergebnis einer Manipulation oder einen beiläufigen Nebeneffekt der Technologie darstellen darf.[242] Darüber hinaus muss es sich um eine „wirksame" technische Maßnahme handeln. Wirksam in diesem Sinne ist eine technische Schutzmaßnahme, wenn deren Umgehung zwar technisch möglich ist, aber einem ohne spezielle technische Kenntnisse ausgestatteten „Durchschnittsbenutzer" erhebliche Schwierigkeiten bereiten würde.[243] Die technische Maßnahme muss zum Zwecke des Schutzes eines urheberrechtlich geschützten Werks oder eines anderen durch das Urheberrecht geschützten Schutzgegenstandes eingesetzt werden.[244]

Zur Verwirklichung des Tatbestands reicht die bloße Ausschaltung der technischen Schutzmaßnahme aus, d.h. jedes Verhalten, das die technische Schutzmaßnahmen außer Kraft setzt.[245] Darüber hinaus ist nicht erforderlich, dass eine urheberrechtlich relevante Handlung wie beispielsweise eine unerlaubte Vervielfältigung in Bezug auf das durch die technische Schutzmaßnahme geschützte Multimediawerk im Anschluss an die Umgehung vorgenommen wird.[246] Das Umgehungsverbot greift somit auch ein, wenn der Nutzer die Umgehungshandlung zum Zwecke der Vornahme einer durch eine urheberrechtliche Schrankenbestimmung legitimierten Handlung begeht.[247] Insoweit gewährt das Gesetz einen vom eigentlichen Schutzumfang des Urheberrechts losgelösten, absoluten Schutz der Integrität von technischen Schutzmaßnahmen.[248] Gemäß § 95 a Abs. 1 Hs. 2 UrhG muss dem Handelnden bekannt sein oder hätte ihm den Umständen nach bekannt sein müssen, dass die Umgehung der technischen Schutzmaßnahme zu dem Zweck erfolgt, um Zugang zu einem Werk oder dessen Nutzung zu ermöglichen. Erforderlich ist somit eine auf die urheberrechtliche Nutzung gerichtete Umgehungsabsicht.[249] Darüber hinaus ist jedoch nicht Voraussetzung, dass seitens des Handeln-

242 *Dreier* s.o.; *Czychowski*, in *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 95 a Rn. 12.

243 *Dreier*, ZUM 2002, 28, 36; *Schippan*, ZUM 2003, 378, 386; *Spindler*, GRUR 2002, 105, 116; *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 34 Rn. 12; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 95 a Rn. 15.

244 *Blocher*, in: *Roßnagel*, Digitale Rechteverwaltung, 2009, S. 43; *Dreyer*, in: *Pahlow/Eisfeld*, 2008, S. 221, 229. Die Umgehung einer technischen Maßnahme zum Schutz eines gemeinfreien Werk würde somit von § 95 a UrhG nicht erfasst, vgl. *Arlt*, GRUR 2004, 548, 550.

245 *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 34 Rn. 15; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 95 a Rn. 10.

246 *Dreyer*, in: *Pahlow/Eisfeld*, 2008, S. 221, 223; *Grützmacher*, in: *Lehmann/Meents* (Hrsg.), FA IT-Recht, Kap. 18, Rn. 254.

247 *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 34 Rn. 4: „relativer Vorrang der technischen Maßnahmen vor den Schranken des Urheberrechts"; *Götting*, in: *Schricker* (Hrsg.), Urheberrecht, 2006, § 95 a Rn. 5.

248 *Arlt*, GRUR 2004, S. 548, 550; a.A. *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 34 Rn. 3, der davon ausgeht, dass die „ergänzenden Schutzbestimmungen" gem. § 95 a UrhG nur auf technischer Ebene die urheberrechtlichen Befugnisse abbilden und daher auf deren Umfang beschränkt sind.

249 *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 34 Rn. 16.

den auch ein Verschulden, d.h. ein fahrlässiges oder vorsätzliches Verhalten vorliegt.[250]

Über den reinen Umgehungsschutz und damit über die Vorgaben der WIPO-Internetverträge hinaus gewährt Art. 6 Abs. 2 Multimediarichtlinie einen Schutz gegen Vorfeldmaßnahmen ähnlich wie 17 U.S.C. § 1201, der in Form von § 95 a Abs. 3 UrhG in deutsches Recht umgesetzt wurde.[251] Hierdurch werden auch vorbereitende Handlungen wie beispielsweise die Herstellung oder Vermarktung von Produkten oder Dienstleistungen, die hauptsächlich zum Zweck der Umgehung hergestellt oder erbracht werden, von dem Umgehungsverbot erfasst.[252]

bb. Durchsetzung von Schrankenbestimmungen gem. Art. 6 Abs. 4 Multimediarichtline bzw. § 95 b UrhG

In Art. 6 Abs. 4 greift die Multimediarichtlinie das Risiko auf, dass durch eine einseitige Ausgestaltung von technischen Schutzmaßnahmen zugunsten der Rechtsinhaber der nach den Urheberrechtsgesetzen der Mitgliedstaaten vorgesehene Ausgleich der Interessen der Rechtsinhaber und der Nutzer von urheberrechtlich geschützten Werken ausgehöhlt werden könnte. Es sollte daher ein Gegengewicht gegen den umfassenden Rechtsschutz für technische Schutzmaßnahmen geschaffen werden.[253] Insoweit setzt die Multimediarichtlinie vorwiegend darauf, dass seitens der Rechtsinhaber freiwillige Maßnahmen ergriffen werden, um die Ausübung von Schrankenbestimmungen in angemessenem Umfang zu gewährleisten.[254] Hierdurch soll verhindert werden, dass durch eine zu weitgehende Aufweichung des Rechtsschutzes für technische Schutzmaßnahmen die Gefahr der Internetpiraterie wieder vergrößert wird.[255] Nur dann, wenn es nicht zu solchen freiwilligen Maßnahmen kommt, sieht die Multimediarichtlinie eine Pflicht der Mitgliedstaaten zur Ergreifung von Maßnahmen vor, durch die sichergestellt wird, dass den Nutzern von den Rechtsinhabern Mittel zur Ausübung von Schrankenbestimmungen auch tatsächlich zur Verfügung gestellt werden.[256] Nicht festgelegt wurde in der Multimediarichtlinie, wie diese Maßnahmen im Einzelnen auszusehen haben.[257]

250 BGH vom 17.07.2008, NJW 2008, 3565 – *Clone-CD*.
251 *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 34 Rn. 18 ff.; *Czychowski*, in *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 95 a Rn. 44 ff.
252 *Dreier*, ZUM 2002, 28, 36; *Arlt*, GRUR 2004, 548, 550.
253 Vgl. hierzu zustimmend *Bayreuther*, ZUM 2001, 828, 838; *Dreier*, ZUM 2002, 28, 37; krit. *Schippan*, ZUM 2003, 378, 386.
254 *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 36 Rn. 3.
255 *Bayreuther*, ZUM 2001, 828, 838.
256 *Dreier*, ZUM 2002, 28, 37; *Reinbothe*, ZUM 2002, 43, 47.
257 *Spindler*, GRUR 2002, 105, 117.

Allerdings gilt die Einschränkung des Rechtsschutzes für technische Schutzmaßnahmen gemäß Art. 6 Abs. 4 Multimediarichtlinie nicht generell für sämtliche Schrankenbestimmungen, die das jeweilige mitgliedstaatliche Urheberrecht vorsieht. Vielmehr wird die Durchsetzbarkeit nur in Bezug auf eine begrenzte Anzahl bestimmter Schrankenbestimmungen gewährt.[258] Darüber hinaus ist Art. 6 Abs. 4 Multimediarichtlinie nicht anwendbar, wenn der Rechtsinhaber sein Werk im Internet „interaktiv" zum Abruf zur Verfügung stellt, der Abruf auf vertraglicher Grundlage erfolgt und im Vertrag nichts Abweichendes vereinbart ist. Da letztere Konstellation in der weit überwiegenden Zahl der Fälle des Konsums von Multimediawerken über das Internet gegeben sein dürfte, wird hierdurch die Anwendbarkeit von Art. 6 Abs. 4 Multimediarichtlinie und damit der darin zum Ausdruck kommende Schutz für überwiegende Gemeinwohlinteressen erheblich geschmälert.[259]

Entsprechend dieser Vorgaben beschränkt § 95 b UrhG den Anwendungsbereich von § 95 a UrhG betreffend die Ausübung der allgemeinen urheberrechtlichen Schrankenbestimmungen gemäß §§ 44 a ff. UrhG nicht unmittelbar.[260] Vielmehr wird den Rechtsinhabern eine durch die Nutzer einklagbare Pflicht auferlegt, urheberrechtlich relevante Handlungen, die durch bestimmte, in der Vorschrift einzeln aufgeführte Schrankenbestimmungen legitimiert sind, in Bezug auf urheberrechtlich geschützte digitale Multimediawerke technisch zu ermöglichen.[261] Der Rechtsinhaber muss somit angemessene Mittel zur Verfügung zu stellen, mit deren Hilfe der Nutzer von einer Schrankenbestimmung in erforderlichem Umfang Gebrauch machen kann.[262] Falls der Rechtsinhaber gegen diese Verpflichtung verstößt, kann er vom Nutzer gemäß § 95 b Abs. 2 UrhG gerichtlich auf die Zurverfügungstellung solcher Mittel in Anspruch genommen werden, gemäß § 2 a UKlaG auch im Wege einer Verbandsklage. Dieser Anspruch gegen den Rechtsinhaber besteht unabhängig davon, ob diesen in Bezug auf sein Versäumnis ein Verschulden trifft. Über dieses einklagbare subjektive Recht[263] hinaus wird den Nutzern

258 *Dreier*, ZUM 2002, 28, 37.
259 *Bayreuther*, ZUM 2001, 828, 838; *Dreier*, ZUM 2002, 28, 37.
260 *Grützmacher*, in: *Lehmann/Meents* (Hrsg.), FA IT-Recht, Kap. 18, Rn. 265. Eine unmittelbare Beschränkung des Anwendungsbereichs von § 95 a UrhG ist lediglich in Bezug auf die Aufgaben und Befugnisse öffentlicher Stellen zum Zwecke des Schutzes der öffentlichen Sicherheit oder der Strafrechtspflege vorgesehen, vgl. § 95 a Abs. 2 UrhG.
261 *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 36 Rn. 13; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 95 b Rn. 22.
262 *Grützmacher*, in: *Lehmann/Meents* (Hrsg.), FA IT-Recht, Kap. 18, Rn. 266; *Blocher*, in: *Roßnagel*, Digitale Rechteverwaltung, 2009, S. 45; *Arlt*, GRUR 2004, 548, 550; *Czychowski*, in *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 95 a Rn. 15 ff.
263 *Lauber/Schwipps*, GRUR 2004, 293, 300; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 95 b Rn. 5; *Czychowski*, in *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 95 b Rn. 5.

jedoch kein Recht auf Selbsthilfe („right to hack“) gegenüber dem Rechtsinhaber eingeräumt.[264]

b. Der Schutz von *copyright management information* gem. Art. 7 Multimediarichtlinie bzw. § 95 c UrhG

In Art. 7 Multimediarichtlinie ist der Schutz von *copyright management information* in enger Anlehnung an den Wortlaut der WIPO-Verträge detailliert geregelt.[265] Diese Vorgaben wurden in § 95 c UrhG weitgehend deckungsgleich in das deutsche Recht übernommen.

Demnach ist es verboten, von Rechtsinhabern stammende „Informationen für die Rechtewahrnehmung“, die an einem Werk oder einem sonstigen urheberrechtlichen Schutzgegenstand angebracht sind oder im Zusammenhang damit erscheinen, zu entfernen oder zu verändern.[266] Informationen für die Rechtewahrnehmung sind gemäß § 95 c UrhG „elektronische Informationen, die Werke oder andere Schutzgegenstände, den Urheber oder jeden anderen Rechtsinhaber identifizieren“ bzw. „Informationen über die Modalitäten und Bedingungen für die Nutzung der Werke oder Schutzgegenstände sowie die Zahlen und Codes, durch die derartige Informationen ausgedrückt werden“. Von dieser Definition erfasst werden sowohl einfache Angaben über den Urheber wie auch digitale Wasserzeichen[267] oder aber bestimmte Standards, wie beispielsweise die „International Standard Book and Serial Numbers“ (ISBN/ISSN) oder der „International Standard Recording Code („ISRC“) der Musikindustrie.[268] Die Informationen müssen vom Rechtsinhaber stammen, d.h. auf ihn zurückzuführen sein.[269] Weiterhin müssen sie mit dem Werk physisch verbunden sein, d.h. entweder an dem Vervielfältigungsstück angebracht

264 *Blocher*, in: *Roßnagel*, Digitale Rechteverwaltung, 2009, S. 45; *Dreier*, ZUM 2002, 28, 38; *Spindler*, GRUR 2002, 105, 117: Ein solches Selbsthilferecht wäre nicht mit dem klaren Wortlaut der Multimediarichtlinie vereinbar, wonach nur die Rechtsinhaber zur Einhaltung der ihnen in Bezug auf die Respektierung von Schrankenbestimmungen auferlegten Verpflichtung gezwungen, nicht aber die Nutzer zu Maßnahmen autorisiert werden können, sich selbst gegen eine Einschränkung ihrer Rechte gegenüber dem Rechtsinhaber zur Wehr zu setzen. – Generell werden die Regelungen betreffend die Ausübung von Schrankenbestimmungen nach der Multimediarichtlinie und ihre Umsetzung durch den Ersten Korb als zu kompliziert und nicht praktikabel kritisiert, vgl. *Götting,* in: *Schricker* (Hrsg.), UrhR, 2006, vor §§ 95 a ff., Rn. 16; *Dreyer*, in: *Pahlow/Eisfeld*, 2008, S. 221, 222; *Czychowski*, in *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 95 b Rn. 2.

265 *Dreier*, ZUM 2002, 28, 39.

266 Vgl. hierzu weiterführend *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006.

267 Vgl. 4. Kapitel, Teil B.II.2.

268 *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 95 c Rn. 7.

269 *Czychowski*, in *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 95 c Rn. 19.

sein oder im Zusammenhang mit seiner öffentlichen Wiedergabe erscheinen.[270] Werke, deren Informationen für die Rechtewahrnehmung im Sinne der Vorschrift manipuliert wurden, dürfen gemäß § 95 c Abs. 3 UrhG auch nicht in Verkehr gebracht werden.[271]

Die relevanten Tatbestandshandlungen müssen objektiv ohne Erlaubnis des Rechtsinhabers erfolgt sein.[272] Auf subjektiver Ebene muss der Handelnde Kenntnis von der Tatsache der fehlenden Erlaubnis gehabt haben.[273] Weiterhin muss dem Handelnden bekannt sein bzw. hätte ihm aufgrund der Umstände jedenfalls bekannt sein müssen, dass er hierdurch die Verletzung von Urheberrechten oder verwandten Schutzrechten veranlasst, ermöglicht, erleichtert oder verschleiert.[274] Durch diese subjektive Voraussetzung wird sichergestellt, dass nur Manipulationshandlungen im Zusammenhang mit einem urheberrechtlich relevanten Verhalten durch die Vorschrift erfasst werden.[275]

c. Rechtsfolgen eines Verstoßes gegen §§ 95 a, 95 c UrhG

Die Multimediarichtlinie lässt offen, welche rechtlichen Folgen sich aus einem Verstoß gegen das Verbot der Umgehung technischer Schutzmaßnahmen sowie der Manipulation von *copyright management information* ergeben müssen.[276] Gefordert wird lediglich, dass die Mitgliedstaaten insoweit einen „angemessenen" Rechtsschutz gewähren müssen,[277] was nach Art. 8 Abs. 2 Multimediarichtlinie bedeutet, dass die Mitgliedsstaaten mindestens Ansprüche auf Schadensersatz, Unterlassungsansprüche sowie – im Zusammenhang mit dem Schutz gegen Vorfeldmaßnahmen gemäß Art. 6 Abs. 2 Multimediarichtlinie – die Möglichkeit der Beschlagnahme von rechtswidrigem Material vorsehen müssen. Rein strafrechtliche oder öffentlich-rechtliche Sanktionen reichen somit nicht aus.[278] Verstöße ziehen daher neben den straf- und bußgeldrechtlichen Sanktionen gemäß §§ 108 b,

270 *Czychowski*, in *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 95 c Rn. 20; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 95 c Rn. 4.
271 *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, S. 201; *Czychowski*, in *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 95 c Rn. 26.
272 *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 35 Rn. 12; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 95 c Rn. 4.
273 *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, S. 204; *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 35 Rn. 14.
274 *Peukert*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 35 Rn. 14; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 95 c Rn. 5.
275 *Arlt*, DRMS, 2006, S. 146; *Czychowski*, in *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 95 c Rn. 21.
276 *Spindler*, GRUR 2002, 105, 116.
277 *Dreier*, ZUM 2002, 28, 39.
278 *Spindler*, GRUR 2002, 105, 119.

111 a UrhG auch Unterlassungs- und Schadensersatzansprüche gemäß §§ 823 Abs. 2, 1004 BGB nach sich, da §§ 95 a, 95 c UrhG Schutzgesetze darstellen.[279]

E. Zwischenergebnis

DRM-Systeme ermöglichen die Verwaltung von Rechtspositionen an digitalen Multimediawerken, indem sie Eingriffe in die Rechtspositionen der Rechtsinhaber durch die Nutzer verhindern können. DRM-Systeme bestehen aus einer Vielzahl unterschiedlicher technischer Komponenten in Abhängigkeit von dem Geschäftsmodell, innerhalb dessen sie eingesetzt werden. Vor dem Hintergrund der Digitalisierung und der Internetpiraterie sowie dem damit einhergehenden Verlust der Kontrolle über tradierte Vertriebswege verbindet sich aus ökonomischer Sicht mit DRM-Systemen die Hoffnung der Multimediaindustrie, durch deren Einsatz die Kontrolle über die Vertriebswege im digitalen Umfeld wiederherzustellen und damit auch im Zeitalter der Digitalisierung an den tradierten Geschäftsmodellen der analogen Welt weiter festzuhalten zu können. DRM-Systeme dienen somit im Ergebnis dazu, die tatsächlichen Voraussetzungen dafür zu schaffen, um die Rechtspositionen der Rechtsinhaber an digitalen Multimediawerken im digitalen Zeitalter auf die gleiche Art und im gleichen Umfang zu kommerzialisieren zu können wie im analogen Zeitalter.

Darüber hinaus werden DRM-Systeme auch durch gesetzliche Maßnahmen auf internationaler und nationaler Ebene geschützt. Das Ziel der Aufrechterhaltung der tradierten Vertriebswege haben sich somit die nationalen Gesetzgeber zueigen gemacht und zu einem Anliegen des Gemeinwohls erhoben. Damit wurden jedoch von gesetzgeberischer Seite von vornherein keinerlei Anreize gesetzt, für die neue Welt der digitalen Technologien und des Internets innovative Ansätze zur Durchsetzung und Kommerzialisierung von urheberrechtlichen Rechtspositionen zu entwickeln. Vielmehr wurde der Versuch der Multimediaindustrie, tradierte Geschäftsmodelle ungeachtet der neuen Gegebenheiten in das Zeitalter der Digitalisierung zu übertragen, gesetzlich legitimiert.[280]

279 BGH vom 17.07.2008, NJW 2008, 3565 – *Clone-CD*; LG München I vom 14.11.2007, ZUM-RD 2008, 97, 100; *Grützmacher*, in: *Lehmann/Meents* (Hrsg.), FA IT-Recht, Kap. 18, Rn. 271; *Czychowski*, in *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 95 a Rn. 51; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 95 a Rn. 5 und § 95 c Rn. 3.

280 So auch *Montagnani*, 26 Cardozo Arts & Ent. L.J. 719, 741, 771 (2009); *Perritt*, 16 Mich. St. J. Int'l Law 113, 122 (2007).

5. Kapitel: Das Scheitern von DRM-Systemen beim Vertrieb von Musik-Downloads über das Internet

In diesem Kapitel wird der Niedergang von DRM-Systemen beim Vertrieb von Musikdownloads über das Internet sowie die Gründe, die hierzu geführt haben, dargestellt.

A. Fakten

> „Imagine a world where every online store sells DRM-free music encoded in open licensable formats. In such a world, any player can play music purchased from any store, and any store can sell music which is playable on all players."[281]

„Kopierschutz ist tot" – so oder ähnlich lauteten Anfang 2008 die Überschriften zahlreicher Artikel und Einträge in einschlägigen Technologie-Weblogs im Internet.[282] Auslöser hierfür war vor allem die Entscheidung von Sony, sein gesamtes Musikrepertoire ab sofort in den USA über den Internethändler Amazon.MP3 als DRM-freie Downloads zu vertreiben, d.h. in Form von Musikdateien im MP3-Format ohne Einsatz eines DRM-Systems. Damit hatte auch das letzte Tonträgerunternehmen der Major Labels den Einsatz von DRM-Systemen beim Vertrieb von Musikdownloads über das Internet aufgegeben.

Der Niedergang von DRM-Systemen für Musikdownloads hatte sich bereits seit längerem abgezeichnet.[283] Steve Jobs, der Vorstandsvorsitzende des Mischkonzerns Apple Inc.,[284] der mit dem iTunes-Store den Markt für Musikdownloads seit Jahren dominiert, hatte bereits im Februar 2007 in einem offenen Brief an die Tonträgerunternehmen appelliert, den Einsatz von DRM-Systemen für Musikdown-

281 *Jobs*, Thoughts on Music, 06.02.2007, http://www.apple.com/hotnews/thoughtsonmusic/ (zuletzt abgerufen am 01.07.2010).

282 *Patalong*, Kopierschutz ist tot. Amazon komplett DRM-frei, Spiegel Online, 11.01.2008, http://www.spiegel.de/netzwelt/web/0,1518,527992,00.html (zuletzt abgerufen am 01.07.2010); *Anderson*, Music exec: „Music 1.0 is dead", Ars Technica, 26.02.2008, http://arstechnica.com/news.ars/post/20080226-music-exec-music-1-0-is-dead.html (zuletzt abgerufen am 01.07.2010); *Bangeman*, DRM (on music) is dead. Long live DRM (on video)!, Ars Technica, 08.01.2008, http://arstechnica.com/news.ars/post/20080108-drm-is-dead-for-music.html (zuletzt abgerufen am 01.07.2010).

283 *Ohne Autor*, Apple ändert Kurs bei iTunes, 08.01.2009, Frankfurter Allgemeine Zeitung, S. 16; der kopiergeschützte Vertrieb von Musikstücken durch die Musikindustrie sei *„von Anfang an zum Scheitern verurteilt"* gewesen, vgl. *Winkelhage*, Apple macht den Weg frei, Frankfurter Allgemeine Zeitung, 08.01.2009, S. 18.

284 Apple vertreibt sowohl Computer als auch Unterhaltungselektronik (beispielsweise den iPod), Betriebssysteme und Anwendungssoftware.

loads aufzugeben.[285] Ein Hauptgrund für diesen Appell war das zuvor festgestellte Missverhältnis zwischen der Menge an Musikdownloads, die insgesamt über den iTunes-Store verkauft worden waren, und der Datenkapazität der verkauften iPod-Geräte.[286] Kurz darauf gaben Apple und EMI bekannt, dass ab Mai 2007 die Kunden des iTunes-Store sämtliche Musiktitel, die aus dem Katalog von EMI stammten, gegen Zahlung eines Aufpreises DRM-frei erwerben konnten.[287] Im August 2007 folgte Universal mit der Ankündigung, sein Musikrepertoire probeweise bis Ende des Jahres über Großhändler wie Amazon, Google, BestBuy und Wal-Mart sowie über die Webseiten der bei ihm unter Vertrag stehenden Künstler DRM-frei zu vertreiben.[288] Daraufhin nahm im September 2007 der Internetversandhändler Amazon in den USA seine Musiksparte „AmazonMP3"[289] zum Verkauf von DRM-freien Musikdownloads im MP3-Format in Betrieb.[290] Ende 2007 stellte dort auch Warner seinen Musikkatalog DRM-frei zur Verfügung.[291] Anfang Januar 2008 machte dann schließlich auch Sony BMG den Weg zum DRM-freien Vertrieb seines Musikkatalogs über AmazonMP3 frei,[292] nachdem sich das Unternehmen mit den Ergebnissen eines sechsmonatigen Testlaufs mit DRM-freien Downloads zufrieden gezeigt hatte.[293] Damit war AmazonMP3 der erste Internethändler, über den die Musiktitel aller Major Labels als DRM-freie Musikdownloads erworben werden konnten.

Hingegen konnte Apple erst im Januar 2009 auf der MacWorld in San Francisco den DRM-freien Vertrieb des insgesamt etwa zehn Millionen Tonaufnahmen um-

285 *Jobs*, Thoughts on Music, 06.02.2007, http://www.apple.com/hotnews/thoughtsonmusic/ (zuletzt abgerufen am 01.07.2010).

286 Wenn man die Gesamtmenge der über den iTunes-Store verkauften Musikdownloads durch die Anzahl aller jemals verkaufter iPod-Geräte teilte, so konnten von den ca. 20.000 Musikdateien, die bis zu diesem Zeitpunkt auf jedem iPod-Gerät gespeichert werden konnten, höchstens 20 aus dem iTunes-Store stammen; vgl. *Einhorn*, 56 J. Copyright Soc'y, 201, 202 (2008).

287 Pressemitteilung von Apple v. 02.04.2007, http://www.apple.com/pr/library/2007/04/02itunes.html (zuletzt abgerufen am 01.07.2010).

288 Pressemitteilung von Universal Music Group v. 10.08.2007, http://new.umusic.com/News.aspx?NewsId=539 (zuletzt abgerufen am 01.07.2010).

289 In Deutschland ist der amerikanische Dienst nicht abrufbar, vgl. daher die deutsche Seite unter http://www.amazon.de/MP3-Musik-Downloads/b/?node=77195031.

290 *Rosenblatt*, Amazon Launches DRM-Free Music Service, DRM Watch, 27.09.2007, www.drmwatch.com/ocr/article.php/3702096 (zuletzt abgerufen am 01.07.2010).

291 *Heise Online*, Warner-Music-MP3 s ab sofort kopierschutzfrei bei Amazon, 28.12.2007, http://www.heise.de/newsticker/meldung/101099 (zuletzt abgerufen am 01.07.2010).

292 *Heise Online,* Amazon nimmt DRM-freie Musik von Sony BMG ins Angebot, 11.01.2008, http://www.heise.de/newsticker/meldung/101664 (zuletzt aberufen am 01.07.2010); Pressemitteilung von Amazon.com, Inc. vom 10.1.2008, http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1095118&highlight (zuletzt abgerufen am 01.07.2010).

293 *Holahan*, Sony BMG Plans to Drop DRM, businessweek.com, 04.01.2008, http://www.businessweek.com/technology/content/jan2008/tc2008013_398775.htm (zuletzt abgerufen am 01.07.2010).

fassenden Repertoires des iTunes-Store verkünden.[294] Da der iTunes-Store, gemessen an der Zahl der über diese Plattform verkauften Tonaufnahmen, zu diesem Zeitpunkt der weltweit größte Musikhändler sogar noch vor dem Handelsgiganten Wal-Mart war, besiegelte diese Ankündigung den Niedergang von DRM-Systemen im Zusammenhang mit dem Vertrieb von Musikdownloads.[295] Eine frühere Einigung über den DRM-freien Vertrieb über den iTunes-Store war seitens der Major Labels in der Hoffnung herausgezögert worden, die jahrelange Vormachtstellung des iTunes-Store auf dem Markt für legale Musikdownloads dadurch zu schwächen, dass man den mit dem iTunes-Store konkurrierenden Musikhändlern den DRM-freien Vertrieb von Musikdownloads zuerst erlaubte.[296] Dieses Ziel wurde jedoch nicht erreicht, da iTunes auch im August 2009 mit 69 Prozent nach wie vor unangefochten der führende Einzelhändler auf dem US-amerikanischen Markt für Musik-Downloads war, wohingegen beispielsweise der Internetdienst Amazon-MP3 knapp ein Jahr nach seiner Inbetriebnahme nur einen Anteil von acht Prozent auf diesem Markt für sich verbuchen konnte.[297] Allerdings war ein Übereinkommen zwischen Apple und den Major Labels auch deswegen nicht früher zustande gekommen, da Apple nicht bereit war, seine Preispolitik nach den Vorstellungen der Tonträgerunternehmen zu ändern. Erst die Einwilligung von Apple in eine Flexibilisierung der Preise führte daher zu einer Einigung. Fortan müssen Einzeltitel und Alben nicht mehr zum Einheitspreis angeboten werden, sondern ist eine individuelle Preisgestaltung in Abhängigkeit beispielsweise von der Popularität eines Musiktitels möglich.[298]

Im Ergebnis entstehen nunmehr ständig neue Internetdienste, deren Angebot auf dem Vertrieb von DRM-freien Musikdownloads basiert. So bietet auch die Musiksparte des sozialen Netzwerks MySpace seit September 2008 Tonaufnahmen der Major Labels nicht nur zum Abruf als Streams,[299] sondern auch zum käuflichen

294 *Ohne Autor*, Apple ändert Kurs bei iTunes, Frankfurter Allgemeine Zeitung, 08.01.2009, S. 16; *Dettweiler*, Kein Kopierschutz mehr! Na und?, Computer & Internet, FAZ.NET v. 07.01.2009, http://www.faz.net/s/Rub4C34FD0B1A7E46B88B0653D6358499FF/Doc~E044C395EA5DE484BBEA50FC047365D26~ATpl~Ecommon~Scontent.html (zuletzt abgerufen am 01.07.2010); *Heise Online*, Macworld: iTunes-Musik wird vom Kopierschutz befreit, 06.01.2009, http://www.heise.de/newsticker/meldung/121237 (zuletzt abgerufen am 01.07.2010).

295 *Ohne Autor*, Apple ändert Kurs bei iTunes, Frankfurter Allgemeine Zeitung, 08.01.2009, S. 16.

296 *Cheng*, Amazon rounds out DRM-free music offering with Sony BMG, Ars Technica, 10.01.2008, http://arstechnica.com/news.ars/post/20080110-amazon-rounds-out-drm-free-music-offering-with-sony-bmg.html (zuletzt abgerufen am 01.07.2010).

297 *Heise Online*, iTunes dominiert weiter den US-Musikmarkt, 18.08.2009, http://www.heise.de/newsticker/meldung/143708 (zuletzt abgerufen am 01.07.2010).

298 *Ohne Autor*, Apple ändert Kurs bei iTunes, Frankfurter Allgemeine Zeitung , 08.01.2009, S. 16.; *Heise Online*, Auch Musicload will (fast) vollständig auf digitale Rechteverwaltung verzichten, 08.01.2009, http://www.heise.de/newsticker/meldung/121324 (zuletzt abgerufen am 01.07.2010).

299 Vgl. 4. Kapitel, Teil B.III.2.

Erwerb in Form von DRM-freien Musikdownloads an.[300] Der Musikdienst des sozialen Netzwerks Facebook befindet sich mit den Major Labels in Gesprächen über ein ähnliches Projekt.[301] Hingegen findet das Thema DRM im jährlichen Bericht des internationalen Verbands der Musikindustrie („IFPI") des Jahres 2009 kaum noch Erwähnung. Insoweit wird lediglich festgehalten, dass die zunehmende Lizenzierung von Internetdiensten zum Vertrieb von DRM-freien Musikdownloads eine „wichtige Entwicklung" des Jahres 2008 darstelle, darunter insbesondere die Ankündigung von Apple, nach einer Einigung mit den Major Labels nunmehr acht Millionen DRM-freie Musiktitel zu flexiblen Preisen zu vertreiben. Von dieser Entwicklung erwartet die IFPI einen wesentliche Ankurbelung für den Markt für Musikdownloads.[302]

In Deutschland kam diese Entwicklung wie üblich mit einer zeitlichen Verzögerung an. Anfang Januar 2009 verkündete zunächst Apple den DRM-freien Vertrieb von Musikdownloads über den iTunes-Store mit Wirkung auch für Deutschland.[303] Unmittelbar danach erklärte der Musikhändler Musicload,[304] ein Tochterunternehmen der Deutschen Telekom, zukünftig nahezu sein gesamtes über das Internet vertriebene Musiksortiment ebenfalls DRM-frei anzubieten.[305] Beide Unternehmen setzten insoweit den 1. April 2009 als Stichtag, bis zu dem die Musikkataloge umgestellt sein sollten. Ende Januar kam ihnen jedoch noch die große Einzelhandelskette Media Markt zuvor, die bereits zu diesem Zeitpunkt eine Plattform eröffnete, auf der ausschließlich DRM-freie Musikdownloads angeboten wurden;[306] Mitte März folgte die Konzernschwester Saturn mit einem ähnlichen Angebot.[307] Am 1. April 2009 öffnete schließlich auch der deutsche Ableger der Musikplattform AmazonMP3 im Internet erstmals ihre Tore, womit den Nutzern fortan über diese Plattform mehr als fünf Millionen Tonaufnahmen als DRM-freie

300 *Sandoval*, iLike talks download store with music labels, CNET News, 21.07.2009, http://news.cnet.com/8301-1023_3-10292389-93.html?part=rss&tag=feed&subj=News-DigitalMedia (zuletzt abgerufen am 01.07.2010).
301 *Sandoval*, s.o.
302 IFPI Digital Music Report 2009, S. 5: „The move is expected to significantly boost download sales.".
303 *Winkelhage*, Apple macht den Weg frei, Frankfurter Allgemeine Zeitung, 08.01.2009, S. 18.
304 http://www.musicload.de.
305 *Heise Online*, Auch Musicload will (fast) vollständig auf digitale Rechteverwaltung verzichten, 08.01.2009, http://www.heise.de/newsticker/meldung/121324 (zuletzt abgerufen am 01.07.2010).
306 *Heise Online*, Mediamarkt bietet MP3-Songs ohne DRM an, 29.01.2009, http://www.heise.de/newsticker/meldung/126576 (zuletzt abgerufen am 01.07.2010).
307 *Heise Online*, Saturn: 250.000 MP3-Alben für je 5 Euro, 13.03.2009, http://www.heise.de/newsticker/meldung/134533 (zuletzt abgerufen am 01.07.2010).

Musikdownloads im MP3-Format zur Verfügung standen.[308] Weiterhin vertreiben die United-Internet-Töchter GMX.de und WEB.de seit Mai 2009 über ihre Musikplattformen ebenfalls etwa fünf Millionen Tonaufnahmen als DRM-freie Musikdownloads.[309]

B. Hintergründe

Der Einsatz von DRM-Systemen im Bereich der Musikdownloads ist aus mehreren, nachfolgend dargestellten Gründen gescheitert.

I. Fehlender Erfolg beim Kampf gegen die Internetpiraterie

Die Notwendigkeit des Einsatzes von DRM-Systemen im Zusammenhang mit dem Vertrieb von Musikdownloads hatte die Musikindustrie vor allem auch mit dem Kampf gegen die Internetpiraterie begründet. Jedoch zeigte der Einsatz von DRM-Systemen insoweit keine spürbaren Auswirkungen,[310] d.h. die Menge der über Filesharing-Netzwerke und P2P-Software im Internet illegal getauschten Musikdateien konnte dadurch nicht verringert werden.[311]

Der Hauptgrund hierfür ist darin zu sehen, dass CDs, die nach wie vor das dominierende Medium beim Vertrieb von Tonaufnahmen darstellen, seit einiger Zeit

308 Pressemitteilung von amazon.de v. 01.04.2009, http://www.amazon.de/gp/press/pr/20090402/ref=amb_link_82934453_2?pf_rd_m=A3JWKAKR8XB7XF&pf_rd_s=center-1&pf_rd_r=0ZFCNQDAJQTMFJV2JS-S3&pf_rd_t=2701&pf_rd_p=467218133&pf_rd_i=home-2009 (zuletzt abgerufen am 01.07.2010); c't news, Amazon startet MP3-Downloads in Deutschland, 01.04.2009, http://www.heise.de/ct/news/meldung/135554 (zuletzt abgerufen am 01.07.2010).

309 *Heise Online*, United Internet kooperiert mit Amazon MP3, 27.05.2009, http://www.heise.de/newsticker/United-Internet-kooperiert-mit-Amazon-MP3--/meldung/139426 (zuletzt abgerufen am 01.07.2010).

310 *Martin*, 28 Loy. L.A. Ent. L. Rev. 265, 266, 288 (2008); *Harvey*, Single-mother digital pirate Jammie Thomas-Rasset must pay $ 80,000 per song, Times Online, 19.06.2009, http://technology.timesonline.co.uk/tol/news/tech_and_web/article6534542.ece (zuletzt abgerufen am 01.07.2010).

311 *Martin*, 28 Loy. L.A. Ent. L. Rev. 265, 266 (2008); vgl. hierzu auch den Kommentar eines Repräsentanten von Media Defender, einem Unternehmen, das Technologielösungen zum Schutz von Inhalten im Internet anbietet: *„DRM is not an antipiracy tool ... What we've seen in P2P networks is that DRM hasn't slowed it down at all. It takes just one person to crack it and it spreads virally ... DRM and lawsuits haven't changed the population, throughput, or bandwith that is being consumed"*, zitiert bei *Bangeman*, DRM (on music) is dead. Long live DRM (on video)!, Ars Technica, 08.01.2008, http://arstechnica.com/news.ars/post/20080108-drm-is-dead-for-music.html (zuletzt abgerufen am 01.07.2010); sueddeutsche.de, Kleine Preise bei Apple, 17.10.2007, http://www.suedeutsche.de/computer/artikel/605/138322/print.html (zuletzt abgerufen am 01.07.2010).

wieder überwiegend frei von DRM-Systemen, die die freie Vervielfältigung von digitalen Tonaufnahmen verhindern, vertrieben werden.[312] Die auf einer CD gespeicherten Tonaufnahmen können daher von jedem Nutzer ohne großen Aufwand „gerippt", d.h. auf einen Computer übertragen und von dort aus über das Internet weiterverbreitet werden.[313] Es ist daher davon auszugehen, dass die im Internet illegal getauschten Dateien zum weit überwiegenden Teil von „gerippten" CDs stammen. Auch bestehen laut dem kalifornischen Marktforschungsunternehmen BigChampagne LLC, das unter anderem Informationen über den Umfang getauschter Film- und Musikdateien im Internet sammelt, kaum Überschneidungen zwischen Nutzern, die ihre Musik auf Plattformen wie dem iTunes-Store in Form von Musikdownloads käuflich erwerben, und denjenigen, die Musikdateien in illegalen Internettauschbörsen zur Verfügung stellen.[314]

Andererseits gibt es mittlerweile konkrete Anhaltspunkte dafür, dass die Verfügbarkeit von Musiktiteln oder –alben im Internet frei vom Schutz durch DRM-Systeme nicht notwendigerweise einen Einbruch beim Verkauf der physischen Datenträger bedeutet. So stellte die Band „Radiohead" ihr neues Album „In Rainbows" ab Oktober 2007 zunächst für knapp zwei Monate auf ihrer Webseite zum Download als DRM-freie MP3-Datei ihren Fans zur Verfügung. Dabei wurde es den Fans überlassen zu entscheiden, wieviel sie für den Download bezahlen wollten (sogenanntes „tip jar"-Vergütungsmodell).[315] Ab 31. Dezember 2007 begann dann der reguläre Vertrieb des Albums als CD.[316] Mit der Vorabveröffentlichung im

312 Vgl. 4. Kapitel, B.III.1.

313 *Martin*, 28 Loy. L.A. Ent. L. Rev. 265, 292 (2008); *Perritt*, 16 Mich. St. J. Int'l Law 113, 143 (2007); *Rosenblatt*, Amazon Launches DRM-Free Music Service, DRM Watch, 27.09.2007, www.drmwatch.com/ocr/article.php/3702096 (zuletzt abgerufen am 01.07.2010); vgl. insoweit auch *Jobs*, Thoughts on Music, 06.02.2007, http://www.apple.com/hotnews/thoughtsonmusic/ (zuletzt abgerufen am 01.07.2010): *„Why would the Major Labels music companies agree to let Apple and others distribute their music without using DRM systems to protect it? The simplest answer is because DRMs haven't worked, and may never work, to halt music piracy. Though the Major Labels music companies require that all their music sold online be protected with DRMs, these same music companies continue to sell billions of CDs a year which contain completely unprotected music. That's right! No DRM system was ever developed for the CD, so all the music distributed on CDs can be easily uploaded to the Internet, then (illegally) downloaded and played on any computer or player. In 2006, under 2 billion DRM-protected songs were sold worldwide by online stores, while over 20 billion songs were sold completely DRM-free and unprotected on CDs by the music companies themselves. The music companies sell the vast majority of their music DRM-free, and show no signs of changing this behavior, since the overwhelming majority of their revenues depend on selling CDs which must play in CD players that support no DRM system."*.

314 *Rosenblatt*, Is EMI's DRM-Free Strategy Working?, DRM Watch, 08.08.2007, http://www.drmwatch.com/ocr/article.php/3693316 (zuletzt abgerufen am 01.07.2010).

315 *Heise Online*, Fans bestimmen Preis des neuen Radiohead-Albums selbst, 01.10.2007, http://www.heise.de/newsticker/meldung/96828 (zuletzt abgerufen am 01.07.2010).

316 *Heise Online*, Neues Radiohead-Album auf CD und vielleicht bald bei iTunes, 12.12.2007, http://www.heise.de/newsticker/meldung/100481 (zuletzt abgerufen am 01.07.2010).

Internet setzte die Band vor allem auf die hierdurch erzeugten Marketingeffekte. Allerdings wurde die Aktion zunächst mit viel Skepsis betrachtet, die durch eine (von der Band nie bestätigte) Studie befördert wurde, wonach nur knapp 40 Prozent der Nutzer für das Herunterladen des Albums im Durchschnitt ca. US$ 6 bezahlt hätten, hingegen die restlichen Nutzer das Downloadangebot ohne Entrichtung einer Gegenleistung genutzt hätten.[317] Anderen Meldungen zufolge verdiente die Band jedoch durch die ersten 1,2 Millionen Downloads zwischen US$ 6-10 Millionen.[318] Weiterhin belegte das Album weniger als zwei Wochen nach seiner regulären Veröffentlichung den ersten Platz sowohl in den britischen als kurz später auch – mit 122.000 verkauften Tonträgern innerhalb von 11 Tagen – den US-amerikanischen Album-Charts.[319] Damit erreichte die Band zum zweiten Mal in ihrer Bandgeschichte den ersten Platz in den USA, den sie bisher nur mit dem Album „Kid A" im Jahr 2000 erreicht hatte, von dem allerdings in der ersten Woche seiner Veröffentlichung 210.000 Stück verkauft worden waren.[320]

Zudem wird durch den Einsatz von DRM-Systemen das Problem der „analogen Lücke" („analog hole") nicht gelöst. Darunter versteht man das Phänomen, dass jedes Multimediawerk, selbst wenn es durch DRM-Systeme geschützt wird, zu irgendeinem Zeitpunkt für den Nutzer wahrnehmbar gemacht, d.h. auf einem Computermonitor gezeigt oder über Lautsprecher wiedergegeben werden muss.[321] Spätestens zu diesem Zeitpunkt ist es jedoch technisch möglich, eine analoge Kopie des auf diese Weise wahrnehmbar gemachten Multimediawerks herzustellen,[322] welche anschließend wiederum digitalisiert, gespeichert, vervielfältigt und über das Internet verbreitet werden kann. Dies bedeutet, dass, egal in welchem Umfang vorbeugende technische Maßnahmen gegen die nicht-autorisierte Verbreitung von Multimediawerken ergriffen werden, es früher oder später immer wieder zum Auftreten unerlaubt angefertigter digitaler Kopien dieser Werke kommen wird. Daran schließt sich das Problem, dass aufgrund der zunehmenden globalen Vernetzung, insbesondere durch das World Wide Web, eine einzige digitale Kopie eines Multimediawerks ausreicht, um das Werk weltweit zu verbreiten, da insbesondere mit Hilfe von Filesharing-Netzwerken und P2P-Software ein Schneeball-Effekt ausgelöst werden kann, wodurch die Vervielfältigung und Verbreitung einer digitalen

317 *Rosenblatt*, Radiohead Takes the Lead in Race to the Bottom, DRM Watch, 08.11.2007, www.drmwatch.com/ocr/article.php/3710021 (zuletzt abgerufen am 01.07.2010).

318 *van Buskirk*, Estimates: Radiohead Made Up To $10 Million on Initial Album Sales (Updated), WIRED, 19.10.2007, http://www.wired.com/listening_post/2007/10/estimates-radio/ (zuletzt abgerufen am 01.07.2010).

319 *Heise Online*, Radiohead-Album erobert auch Platz 1 der US-Charts, 11.01.2008, http://www.heise.de/newsticker/meldung/101638 (zuletzt abgerufen am 01.07.2010).

320 *Lee*, 2008 U. Ill. L. Rev. 1459, 1503 (2008).

321 *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, S. 22.

322 Beispielsweise durch Abfilmen der angezeigten Bilder mit einer Videokamera oder durch Aufzeichnung des über die Lautsprecher der Stereoanlage wiedergegebenen Tonaufnahme auf Tonband.

Kopie innerhalb kürzester Zeit „explodieren", d.h. massenweise auftreten kann.[323] Ebenso bedarf es nur eines einzigen technisch versierten Nutzers, der sich das „Knacken" eines DRM-Systems zur Aufgabe macht, um das DRM-System in seiner Wirksamkeit wesentlich zu beeinträchtigen, da auch dieser Nutzer die Möglichkeit hat, das von ihm entwickelte Werkzeug zur Außerkraftsetzung des DRM-Systems innerhalb kürzester Zeit über das Internet weltweit zu verbreiten.[324]

II. Beeinträchtigung der Nutzerinteressen

Ein wesentlicher Faktor für das letztendliche Scheitern von DRM-Systemen im Zusammenhang mit Musikdownloads liegt darin, dass die Nutzung von DRM-geschützten Musikdateien mit mehreren erheblichen Nachteilen für deren Nutzer einhergeht, die nachfolgend unter den Stichworten Interoperabilität, Nachhaltigkeit sowie Daten- und Verbraucherschutz skizziert werden.[325]

1. Interoperabilität

Als einer der größten Nachteile des Vertriebs von digitalen Multimediawerken, die durch DRM-Systeme geschützt werden, hat sich die fehlende Kompatibilität zwischen diesen Systemen und den zu ihrer Nutzung verwendeten digitalen Endgeräten erwiesen (sogenannte „interoperability", nachfolgend Interoperabilität).[326] Die Interoperabilität scheitert oftmals daran, dass die verschiedenen im Rahmen von Internetdiensten, auf physischen Datenträgern und in digitalen Endgeräten eingesetzten DRM-Systeme nicht miteinander kommunizieren und arbeiten können. Dieser Nebeneffekt von DRM-Systemen hat speziell im Musikbereich auf Seiten der Nutzer zu großer Frustration geführt.[327]

323 *Haber/Horne/Pato/Sander/Tarjan*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 224, 230; *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, S. 22.

324 *Haber/Horne/Pato/Sander/Tarjan.*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 224, 230; *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, S. 22; vgl. zu diesem sog. „darknet effect" auch *Biddle/England/Peinado/Willman*, The Darknet and the Future of Content Distribution, abrufbar unter http://msl1.mit.edu/ESD10/docs/darknet5.pdf (zuletzt abgerufen am 01.07.2010.).

325 Vgl. *Rohleder*, ZUM 2003, 203, 204, der die Benutzerfreundlichkeit von DRM als *„erfolgskritische[n] Faktor"* bezeichnet.

326 *Castro/Bennett/Andes*, Steal These Policies, ITIF, 2009, S. 8; *Reinke*, Wertschöpfungsmöglichkeiten Musikindustrie, 2009, S. 44.

327 *Samuelson/Schultz*, 6 J. Telecom. & High Tech. L. 41, 49 (2007); vgl. auch *Patalong*, Kopierschutz ist tot. Amazon komplett DRM-frei, Spiegel Online, 11.01.2008, www.spiegel.de/netzwelt/web/0,1518,527992,00.html (zuletzt abgerufen am 01.07.2010); *Roth*, 18 Fordham Intell. Prop. Media & Ent. L.J. 515, 522 (2008).

Die Kompatibilität verschiedenster digitaler Endgeräte, Formate, Plattformen und Applikationen, der sogenannte „Netzwerkeffekt", gilt als eine der größten Errungenschaften der Digitalisierung, die den Nutzern von Computern, digitalen Endgeräten und Internet eine Fülle neuer Möglichkeiten im Umgang mit digitalen Inhalten ermöglichen.[328] Die Nutzung dieses Netzwerkeffekts hängt jedoch maßgeblich davon ab, dass der Austausch von Daten zwischen den verschiedenen Geräten und Anwendungen möglichst reibungslos funktioniert[329] und in diesem Zusammenhang auch keine größeren Kosten beispielsweise für die Herstellung der notwendigen Kompatibilität entstehen („Transaktionskosten"). Der Einsatz nichtinteroperabler DRM-Systeme führt jedoch gerade zum gegenteiligen Effekt, nämlich der Einschränkung der Kompatibilität von Geräten und Anwendungen, und damit zu einer Beeinträchtigung des Netzwerkeffekts sowie zu einer Erhöhung der Transaktionskosten, da zusätzliche Maßnahmen erforderlich werden, um die durch DRM-Systeme hervorgerufenen Beeinträchtigungen des effizienten Datenaustausches wieder zu beseitigen.[330] Damit wird jedoch einer der größten Vorteile der Digitalisierung durch den Einsatz von DRM-Systemen konterkariert.[331]

Im Zusammenhang mit Musikdownloads wurde die fehlende Interoperabilität von DRM-Systemen bisher von den Anbietern von Onlineshops bewusst dazu eingesetzt, um die Kompatibilität von über das Internet erworbenen Tonaufnahmen mit Abspielgeräten und Internetangeboten konkurrierender Anbieter einzuschränken und hierdurch die Nutzer stärker an den eigenen Dienst und die zugehörigen Geräte zu binden.[332] So wurde durch das von Apple entwickelte DRM-System FairPlay sichergestellt, dass über den iTunes-Store erworbene digitale Tonaufnahmen nicht auf jedem MP3-Player, sondern nur auf dem von Apple entwickelten

328 *Samuelson/Schultz*, 6 J. Telecom. & High Tech. L. 41, 47 (2007).

329 *Vinje*, EIPR 1996, 431, 437.

330 *Samuelson/Schultz*, 6 J. Telecom. & High Tech. L. 41, 47 (2007); *Hansen*, Gesprengte Ketten – Legale MP3-Downloads in Deutschland, c't 2009, Heft 9, S. 136 ff. Konkret bedeutet die durch DRM-Systeme herbeigeführte Erhöhung der Transaktionskosten durch mangelnde Interoperabilität beispielsweise für den Online-Händler, dass sich sein Aufwand für die Beantwortung von Kundenanfragen wesentlich erhöht, wenn sich nach dem Erwerb digitaler Inhalte die Beschwerden der Erwerber über technische Schwierigkeiten bei deren Nutzung häufen; für den Nutzer stellt der Erwerb des digitalen Inhalts eine Fehlinvestition dar, wenn er diesen auf dem von ihm verwendeten Endgerät nicht nutzen kann; teilweise erhöht sich der Aufwand sogar auf Seiten derjenigen, die durch die DRM-Systeme eigentlich geschützt werden sollen, wenn beispielsweise dem Musiker die Vermarktung seiner Werke erschwert wird, indem die durch das DRM-System errichteten technischen Hürden das Einstellen von Werken auf eine Plattform erschweren.

331 *Fetscherin*, in: Becker/Buhse/Günnewig/Rump (Hrsg.), DRM, 2003, S. 305, 319, führt als Beispiel die Veröffentlichung des neuen Albums einer populären Musikkünstlerin (Natalie Imbruglia) auf CD mit einer Kopierschutztechnologie anführt, die zu einer Welle von Beschwerden seitens der Käufer führte, da diese die CD in einigen Endgeräten nicht nutzen konnten; BMG sah sich schließlich gezwungen, das Album nochmals ohne Kopierschutz herauszubringen und die defekten CDs zu ersetzen.

332 *Samuelson/Schultz*, 6 J. Telecom. & High Tech. L. 41, 47 (2007.).

iPod abgespielt werden konnten. Darüber hinaus wurde der iPod so gestaltet, dass Tonaufnahmen, die durch DRM-Systeme anderer Anbieter geschützt werden, hierüber nicht abgespielt werden konnten. Neben den durch die FairPlay-Technologie geschützten Musikdownloads konnten über das Gerät nur Tonaufnahmen in DRM-freien Formaten wie beispielsweise dem MP3-Format genutzt werden. Dies bedeutete jedoch, dass Nutzer, die sich für den iPod entschieden hatten, im Wesentlichen nur den iTunes-Store, nicht aber andere Onlineshops nutzen konnten, sofern diese ein anderes DRM-System als die Fair-Play-Technologien einsetzten. Andererseits blieb es Nutzern, die sich für einen anderen MP3-Player als den iPod entschieden hatten, verwehrt, den Musikkatalog des iTunes-Store, der über lange Zeit das attraktivste, da umfangreichste legale Angebot zum Erwerb von Musikdownloads über das Internet darstellte, mit ihrem Gerät zu nutzen.[333] DRM-Systeme wurden somit dazu instrumentalisiert, Kunden an bestimmte Vertriebswege und Produkte zu binden, um dadurch eine auch unter wettbewerbsrechtlichen Aspekten bedenkliche Abschottung von anderen, konkurrierenden Marktteilnehmern zu erreichen (sogenannter „digitaler lock-in").[334]

Eine Initiative der Tonträgerunternehmen namens „Coral", die darauf gerichtet war, eine bessere Interoperabilität durch die Standardisierung von den im Musikbereich eingesetzten DRM-Systemen zu erreichen, scheiterte im Jahr 2004.[335] Der

333 Vgl. zu dieser Problematik speziell im Hinblick auf das iTunes-iPod-Ecosystem *Sharp/Arewa*, 5 Nw. J. Tech. & Intell. Prop. 332 (2007); *Patalong*, Kopierschutz ist tot - Amazon komplett DRM-frei, Spiegel Online, 11.01.2008, www.spiegel.de/netzwelt/web/0,1518,527992,00.html (zuletzt abgerufen am 01.07.2010); *Winkelhage*, Apple macht den Weg frei, Frankfurter Allgemeine Zeitung, 08.01.2009, S. 18; sowie *Berkman Center for Internet and Society at Harvard Law School*, iTunes: How Copyright, Contract, and Technology Shape the Business of Digital Media – a Case Study, 2004, S. 45, http://cyber.law.harvard.edu/media/uploads/81/iTunesWhitePaper0604.pdf (zuletzt abgerufen am 01.07.2010), worin es hierzu heißt: *„The increased protection that Apple's DRM is able to enjoy as a consequence of the DMCA and the EUCD implementations allows today for the deployment of a market strategy based on excluding competition through restricted interoperability. Assuming for the moment that iTunes Store's main purpose is to generate profits in iPod sales (even if operating at a loss), restricting interoperability is a sound business decision. In making this decision, Apple has to balance the trade-off between the possible increase in profits derived from expanding the iTunes Store's consumer base, and removing the strategic advantage the iPod has by way of its exclusive relationship to the iTunes service. Making iTMS songs exclusively compatible with iPod allows for the generation of noticeable entry barriers in the market of portable players and some barriers in the market of music downloading services (iTMS) competitors."*.

334 *Einhorn*, Gorillas in Our Midst, 2007, S. 10: *"... This may be termed digital "lock-in", which is a critical example of an noncooperative market (or Nash) equilibrium where the "invisible hand" does not bring unalloyed private interests to the most efficient point. ..."*; *Martin*, 28 Loy. L.A. Ent. L. Rev. 265, S. 266, 281ff. (2008); vgl. zusammenfassend zu der kartellrechtlichen Problematik *Roth*, 18 Fordham Intell. Prop. Media & Ent. L.J. 515, 525 (2008); *Perritt*, 16 Mich. St. J. Int'l Law, 113, 137 (2007); *Samuelson/Schultz*, 6 J. Telecom. & High Tech. L. 41, 46 (2007); *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, S. 25 ff.

335 Coral Consortium, http://www.coral-interop.org (zuletzt abgerufen am 01.07.2010).

Grund des Scheiterns lag in den Partikularinteressen der einzelnen Marktteilnehmer, d.h. den gegenläufigen Zielen und Erwartungen von Internetanbietern, Softwareproduzenten und den Herstellern von digitalen Endgeräten. Denn die Motivation, einem einheitlichen Standard für DRM-Systeme zuzustimmen, ist abhängig von der Marktposition des jeweiligen Unternehmens.[336] Verfügt das Unternehmen über einen großen Marktanteil und eine proprietäre DRM-Technologie, so bestehen in der Regel kaum Anreize für die Entwicklung einer interoperablen Technologie, die dazu führen würde, dass seine Kunden leichter zum vergleichbaren Angebot eines Wettbewerbers wechseln könnten. Ein neuer Marktteilnehmer hingegen hat regelmäßig ein hohes Interesse an einheitlichen technologischen Standards, da dies den Markteintritt und den Wettbewerb mit bereits etablierten Marktteilnehmern wesentlich erleichtert.[337]

2. Nachhaltigkeit

Zudem laufen die Nutzer von DRM-geschützten digitalen Multimediawerken, die von einem DRM-System extern betreut werden, das Risiko, dass die Nutzbarkeit dieser Werke nachträglich beschränkt oder gar gänzlich unmöglich wird. Denn solche nachträglichen Änderungen wirken sich über das jeweilige DRM-System, das die in Bezug auf die geschützte Datei vorgenommenen Handlungen fortlaufend verifizieren und autorisieren muss,[338] in der Regel auch auf bereits erworbene digitale Multimediawerke aus.[339]

Dass der Erwerb von durch DRM-Systeme geschützten Musikdateien mit solch gravierenden Nachteilen für die Nutzer einhergehen kann, zeigte sich sehr anschaulich im Jahr 2008, als kurz hintereinander Microsoft, Yahoo und Wal-Mart die Einstellung einiger der von ihnen betriebenen Musikdownload-Angebote ankündigten. Dies bedeutete gleichzeitig, dass die in diesem Zusammenhang eingesetzten DRM-Systeme nicht länger unterstützt werden würden. Damit hätten jedoch die Nutzer ihre über diese Dienste erworbenen Tonaufnahmen ab dem Zeitpunkt ihrer Einstellung nicht mehr auf neue Computer oder andere digitale Endgerät übertragen können, da die zur Autorisierung einer solchen Übertragung erforderlichen Codes durch die jeweiligen DRM-Systeme nicht mehr ausgestellt

336 *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, S. 26; *Perritt*, 16 Mich. St. J. Int'l Law 113, 139-40 (2007).
337 *Perritt*, 16 Mich. St. J. Int'l Law 113, 139 (2007).
338 Vgl. 4. Kapitel, Teil B.I.
339 *Samuelson/Schultz*, 6 J. Telecom. & High Tech. L. 41, 58 (2007).

werden würden.[340] Somit hätten die betroffenen Nutzer die Musikdateien auf legalem Weg zwar wie bisher auf den bereits durch das jeweilige DRM-System autorisierten Geräten abspielen können, nicht hingegen auf nach der Einstellung der DRM-Systeme neu erworbenen Geräten.

Aufgrund der daraufhin einsetzenden massiven Proteste der Nutzer entschieden sich alle Anbieter sukzessive, den Zeitraum, während dessen die DRM-Systeme weiterhin unterstützt werden würden, zu verlängern.[341] Damit wurden die negativen Folgen für die Nutzer zwar nicht beseitigt, jedoch ihr Eintreten zumindest auf einen späteren Zeitpunkt verschoben. Anders im Falle des Internetdienstes SpiralFrog, der seinen Dienst im März 2009 einstellte und dessen Nutzer die über diesen Dienst erworbenen DRM-geschützte Tonaufnahmen bereits kurze Zeit später nicht mehr nutzen konnten.[342]

Als ein weiteres Beispiel für das Problem der Nachhaltigkeit DRM-geschützter Inhalte kann auch Apples iTunes-Store angeführt werden. In seiner kurzen Geschichte hat dieser Dienst bereits mehrere Male seine Nutzungsbedingungen und damit auch die Autorisierung von Nutzerhandlungen durch das DRM-System „Fair Play" geändert, beispielsweise bezüglich der Anzahl erlaubter Kopien oder der Häufigkeit der Übertragung auf weitere digitale Endgeräte.[343]

Im Falle eines digitalisierten Multimediawerks, das ein Nutzer in Form einer DRM-geschützten Datei erwirbt, ist deren dauerhafte Nutzbarkeit von der fortlaufenden Unterstützung durch das DRM-System abhängig. Das funktionsfähige DRM-System ist somit gleichsam die Lebensader des digitalen Multimediawerks. Damit steht und fällt dessen Nutzbarkeit jedoch mit dem Geschäftserfolg und der Geschäftsstrategie des jeweiligen Anbieters, über den das Multimediawerk erworben wird. Denn nur solange der Internetdienst des Anbieters „läuft", wird dieser das von ihm ursprünglich eingesetzte DRM-System technisch unterstützen. Sobald

340 Vgl. zudem die bei *Samuelson/Schultz*, 6 J. Telecom. & High Tech. L. 41, 58-59 (2007) genannten Beispiele für ähnliche Probleme bei der Einstellung des DivX-Systems für Filme sowie sowie des sog. „Sony Connect" Service.

341 *Müller*, Microsoft verlängert DRM für MSN-Music-Songs, iPhone-Welt News, 22.06.2008, http://www.macwelt.de/artikel/_News/356844/microsoft_verlaengert_drm_fuer_msn_music_songs/1 (zuletzt abgerufen am 01.07.2010); *Kane*, Wal-Mart reverses policy on DRM?, CNET News, 10.10.2008, http://news.cnet.com/8301-1023_3-10063168-93.html?tag=mncol;txt (zuletzt abgerufen am 01.07.2010); *Sandoval*, Dear Steve Jobs: Set the music free, CNET News, 20.11.2008, http://news.cnet.com/8301-1023_3-10103484-93.html?part=rss&tag=feed&subj=News-DigitalMedia (zuletzt abgerufen am 01.07.2010).

342 *Sandoval*, SpiralFrog DRM music to play 60 Days, then vanish, CNET News, 20.03.2009, http://news.cnet.com/8301-1023_3-10201355-93.html?part=rss&tag=feed&subj=News-DigitalMedia (zuletzt abgerufen am 01.07.2010).

343 *Samuelson/Schultz*, 6 J. Telecom. & High Tech. L. 41, 58 (2007).

jedoch die Geschäftsstrategie geändert oder der Dienst eingestellt wird, kann dies für den Nutzer bedeuten, dass die von ihm erworbenen Dateien nutzlos werden.[344]

3. Daten- und Verbraucherschutz

Im analogen Zeitalter war es den Rechtsinhabern schlicht nicht möglich, die konkrete Verwendung eines in Form eines physischen Datenträgers durch einen Nutzer erworbenen Multimediawerks nachzuverfolgen.[345] Hingegen ermöglichen es DRM-Systeme, jede Handlung, die ein Nutzer in Bezug auf eine DRM-geschützte Datei vornimmt, zu registrieren und an den das DRM-System betreuenden Server zu kommunizieren, worüber die auf diese Weise erhobenen Daten gespeichert und an Dritte, beispielsweise den Rechtsinhaber, weitergegeben werden können.[346] Dies dient zwar einerseits dem legitimen Interesse des Rechtsinhabers, zu verifizieren, ob ein Nutzer die in Bezug auf ein Multimediawerk geltenden Nutzungsbedingungen einhält. Andererseits können diese Daten auch zu anderen Zwecken genutzt werden, beispielsweise zur Erstellung eines Nutzerprofils, um Werbung individuell auf einzelne Nutzer abzustimmen, oder zum Verkauf an andere Firmen, die an solchen Daten zumeist ebenfalls zu Werbezwecken interessiert sind.[347] Auch besteht zumeist wenig Transparenz darüber, in welchem Umfang und zu welchen Zwecken im Zusammenhang mit der Nutzung eines DRM-geschützten Multimediawerks Daten über den jeweiligen Nutzer erhoben und genutzt werden. Es besteht somit die Gefahr, dass durch den Einsatz von DRM-Systemen die Nutzer zunehmend zu „gläsernen Kunden" werden, deren Konsumverhalten in Bezug auf den Umgang mit digitalen Multimediawerken durch die Anbieter DRM-gestützter Dienste minutiös nachverfolgt werden kann. [348] Der Einsatz von DRM-Systemen weckt daher auch datenschutzrechtliche Bedenken, wegen der Gefahr des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung.[349]

344 *Patalong*, DRM – Musik mit Ablaufdatum, Spiegel Online, 24.04.2008, www.spiegel.de/netzwelt/tech/0,1518,549385,00.html (zuletzt abgerufen am 01.07.2010); s.a. *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, S. 29.

345 *Samuelson/Schultz*, 6 J. Telecom. & High Tech. L. 41, 46 (2007).

346 *Samuelson/Schultz*, s.o.

347 *Samuelson/Schultz*, 6 J. Telecom. & High Tech. L. 41, 51 (2007).

348 Vgl. zu dieser Problematik insbesondere die Studie im Auftrag des Bundesministeriums für Bildung und Forschung „privacy4DRM", an der u.a. das Fraunhofer Institut für Digitale Medientechnologie beteiligt ist, abrufbar unter https://www.datenschutzzentrum.de/drm/privacy4drm.pdf (zuletzt abgerufen am 01.07.2010); weiterhin *Schaar,* Datenschutz im Internet, 2002, Rn. 32 ff.; *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, S. 30; sowie zu den vielfältigen Möglichkeiten zur Datenauswertung und –verwendung im E-Commerce (allerdings ohne spezielle Berücksichtigung von DRM-Systemen) *Roßnagel/Banzhaf/Grimm*, Datenschutz im Electronic Commerce, 2003, S. 55 ff.

349 BVerfG vom 15.12.1983, BverfGE 65, 1.

Auch aus Sicht des Verbraucherschutzes ist der Einsatz von DRM-Systemen nicht unbedenklich, da die an den Computern der Nutzer durch DRM-Technologien herbeigeführten Änderungen auch negative Folgeeffekte nach sich ziehen und schlimmstenfalls sogar zu Schäden an absoluten Rechtsgütern der Nutzer führen können. Bestes Beispiel hierfür ist der Rootkit-Skandal, der eine von Sony (damals noch SonyBMG) im Zusammenhang mit CDs verwendete DRM-Technologie betraf. Mit Hilfe der von Sonys DRM-System verwendeten Software wurde die Nutzbarkeit von auf CD gespeicherten Musikdateien dahingehend eingeschränkt, dass von ihnen nur eine bestimmte Anzahl an Kopien in einem bestimmten, geschützten Format erstellt werden konnten, die wiederum nur auf bestimmten digitalen Endgeräten abgespielt werden konnten.[350] Zu diesem Zweck wurde die Software von den erworbenen CDs automatisch auf die Computer der Käufer aufgespielt und mit Hilfe einer sogenannten „root kit"-Funktion sichergestellt, dass sie nicht mehr von den Computern entfernt werden konnte. Allerdings führte diese Funktion auch zu dem unerwünschten Nebeneffekt, dass die Computer für externe Angriffe auf die darauf gespeicherten Daten anfällig, d.h. leichter zugänglich für Hacker wurden.[351]

Der Rootkit-Skandal zeigt deutlich, dass der Einsatz von DRM-Systemen für die Nutzer in der Regel nicht nur zu erheblichen Nutzungseinschränkungen führt und aus datenschutzrechtlichen Gründen bedenklich ist, sondern darüber hinaus sogar eine Gefahr für sonstige geschützte Interessen des Nutzers, wie beispielsweise die Unversehrtheit des Eigentums darstellen kann.

III. DRM-Systeme als „Paracopyright"

Der Einsatz von DRM-Systemen, gekoppelt mit dem gesetzlichen Schutz vor Umgehung dieser Systeme, versetzt die Rechtsinhaber faktisch in die Lage, die Nutzung digitaler Multimediawerke in einem Maß zu kontrollieren, wie dies weder vom US-amerikanischen noch vom deutsch-europäischen Urheberrecht vorgesehen ist.

350 *Rosch*, 22 Berkeley Tech. L.J. 971, 972 (2007).

351 *Rosch*, s.o. Nach dem Bekanntwerden dieser Sicherheitslücke reichten die betroffenen Käufer Sammelklagen gegen SonyBMG ein. Für eine ausführliche Darstellung des Rootkit-Skandals und seiner Folgen vgl. *Mulligan*/*Perzanowski*, 22 Berkeley Tech. L. J. 1157 (2007). Eine deutsche Klage im Zusammenhang mit diesem Vorfall wurde noch im September 2009 entschieden, vgl. AG Hamburg-Wandsbek, Az. 712 C 113/08.

1. Grundstrukturen des US-amerikanischen und deutsch-europäischen Urheberrechts

a. USA

Das US-amerikanische *copyright law* ist im 17. Titel des United States Code geregelt.[352] Basierend auf der sogenannten „IP clause" der US-amerikanischen Verfassung[353] erließ im Jahr 1790 der Kongress ein für alle Bundesstaaten einheitliches, nationales Urheberrechtsgesetz in Form des *Copyright Act of 1790* („Copyright Act").[354] Dieses Gesetz führte ein zunächst auf vierzehn Jahre begrenztes, um weitere vierzehn Jahre verlängerbares sogenanntes „copyright" für Bücher[355] ein, für dessen Wirksamkeit eine Registrierung beim örtlichen District Court erforderlich war.[356] Dieses *copyright* wurde sukzessive auch bezüglich Druckwerken, musikalischen Kompositionen, Theaterstücken, Fotografien, Kunstwerken und Skulpturen gewährt.[357] Im Rahmen einer grundlegenden Reform des *Copyright Act* im Jahre 1909 wurde das *copyright* für Bücher allgemein auf Schriftwerke erweitert, die Schutzfrist verdoppelt[358] und ein begrenzter Schutz auch für Werke ausländischer Herkunft eingeführt.[359] Im Jahre 1976 wurde der *Copyright Act* wiederum

352 Daher werden einzelne Vorschriften *des Copyright Act* nachfolgend wie folgt zitiert: 17 U.S.C. § 106.

353 Art. 1 § 8 Clause 8: *„Congress shall have the power ... to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries"*.

354 1 Stat. 124 (1790). Aufgrund ihrer Rechtstradition als common law Staaten basierten die meisten der ersten Urheberrechtsgesetze der einzelnen U.S. Bundesstaaten auf dem englischen „Statute of Anne", das vom englischen Parlament im Jahre 1710 verabschiedet worden war. Die Schwierigkeit, diese zum Teil widersprüchlichen Gesetze in grenzüberschreitenden Fällen anzuwenden, führte zu der allgemeinen Überzeugung, dass zur Vereinheitlichung der Rechtsmaterie ein für alle Bundesstaaten gleichermaßen geltendes, nationales Gesetz erlassen werden müsse, vgl. *Merges/Menell/Lemley*, Intellectual Property, 2003, S. 321.

355 Darüber hinaus erstreckte sich der Urheberrechtsschutz auf Landkarten und grafische Darstellungen.

356 *Merges/Menell/Lemley*, Intellectual Property, 2003, S. 321.

357 *Merges/Menell/Lemley*, s.o.

358 Mittlerweile dauert die Schutzfrist des copyright in Bezug auf Werke, die am 01.01.1978 oder später erschaffen wurden, vom Zeitpunkt der Erschaffung des Werks über die gesamte Lebenszeit des Urhebers bis siebzig Jahre über dessen Tod hinaus, vgl. 17 U.S.C. § 302(a); im Falle einer *work made for hire* läuft die Schutzfrist für fünfundneunzig Jahre ab dem Zeitpunkt der ersten Veröffentlichung des Werkes bzw. einhunderzwanzig Jahre ab Erschaffung des Werks, je nachdem, welches dieser beiden Ereignisse zuerst eintritt, vgl. 17 U.S.C. § 302(c).

359 *Merges/Menell/Lemley*, Intellectual Property, 2003, S. 322.

reformiert, wodurch das Gesetz weitgehend seine gegenwärtige Form fand,[360] auch wenn es seither noch etliche Male geändert wurde.[361]

Ein *copyright* wird in Bezug auf „original works of authorship" gewährt, d.h. in Bezug auf ein durch einen Urheber unabhängig erschaffenes Werk, das ein Mindestmaß an Kreativität aufweist und von dem Urheber auf eine Weise fixiert wurde, die eine längere als bloß vorübergehende Wahrnehmung, Wiedergabe oder anderweitige Kommunikation dieses Werks ermöglicht.[362] Die einem Werk unterliegende Idee ist im Gegensatz zu der konkreten Ausdrucksform, die diese Idee in dem Werk des Urhebers gefunden hat, nicht schutzfähig („idea-expression dichotomy").[363] Als originärer Urheber („author") gilt grundsätzlich derjenige, der das betreffende Werk selbst erschaffen hat.[364] Eine Ausnahme gilt im Falle sogenannter „works made for hire", bei denen nicht der Erschaffer des Werks, sondern der Arbeitgeber, in dessen Auftrag und auf dessen Kosten das Werk angefertigt wurde, als dessen Urheber gilt. Daher können auch Unternehmen Inhaber eines *copyright* sein.

Eine Besonderheit des US-amerikanischen Urheberrechts ist die freie Übertragbarkeit des *copyright* in seiner Gesamtheit. Daneben ist auch eine teilweise Übertragung einzelner durch das *copyright* in Bezug auf ein Werk gewährte Rechtspositionen möglich.[365] Dem Inhaber eines *copyright* wird anders als im deutschen Recht[366] kein subjektives Ausschließlichkeitsrecht,[367] sondern lediglich ein Bündel bestimmter Verwertungsrechte gewährt,[368] die allein der Urheber oder ein durch

360 Copyright Act of 1976, Pub. L. No. 94-553, 90 Stat. 2541.

361 1980 wurden aufgrund der im Bericht der „National Comission on New Technological Uses of Copyright" (CONTU) ausgesprochenen Empfehlungen Computerprogramme ausdrücklich in den Geltungsbereich des Gesetzes einbezogen (vgl. 17 U.S.C. §§ 101, 117). Aufgrund des Beitritts der USA zur RBÜ folgte 1988 die Abschaffung einiger Formvorschriften, insbesondere der Kennzeichnungspflicht („notice"), sowie 1990 die Einführung des sogenannten *Architectural Works Copyright Protection Act*. 1998 wurde durch den sogenannten *Sonny Bono Copyright Term Extension Act* die Schutzfrist für Urheberrechte um 20 Jahre verlängert. Durch den sogenannten *Audio Home Recording Act* von 1992 („AHRA") sowie den DMCA (vgl. 4. Kapitel, Teil D.II.1) 1998 wurde das Gesetz an die Herausforderungen durch technische Neuentwicklungen im Bereich der Unterhaltungselektronik (AHRA) sowie die Digitalisierung und das Internet (DMCA) angepasst.

362 Vgl. 17 U.S.C. § 102(a).

363 Vgl. 17 U.S.C. § 102(b). Alle Werke, die vor dem Jahr 1989 erschaffen wurden, müssen zudem mit einem Hinweis auf ihren urheberrechtlichen Schutz gekennzeichnet sein; diese sog. „copyright notice" ist weithin bekannt in Form des ©-Symbols. Darüber hinaus ist eine Eintragung des Urheberrechts beim U.S. Copyright Office keine Wirksamkeitsvoraussetzung mehr für die Entstehung des *copyright*. Jedoch ist eine Registrierung weiterhin erforderlich, wenn ein Rechtsinhaber vor Gericht eine Klage wegen Verletzung eines *copyright* erheben will (vgl. 17 U.S.C. § 411).

364 Vgl. 17 U.S.C. § 201.

365 Vgl. 17 U.S.C. § 201(d).

366 Vgl. 5. Kapitel, Teil B.III.1.b.

367 *Wand*, Technische Schutzmaßnahmen, 2001, S. 230.

368 *Reese*, 34 Sw. U. L. Rev. 287, 289 (2004).

Rechtsübertragung oder Bevollmächtigung legitimierter Dritter auszuüben berechtigt ist. Diese Verwertungsrechte bestehen in der exklusiven Berechtigung, ein Werk zu vervielfältigen, zu bearbeiten, zu verbreiten, öffentlich auszustellen oder öffentlich aufzuführen.[369]

Wird eines dieser Rechte ohne die Erlaubnis des Rechtsinhabers ausgeübt, so liegt eine Urheberrechtsverletzung („copyright infringement") gemäß 17 U.S.C. § 501(a) vor. Da es sich bei der Haftung für Urheberrechtsverletzungen um eine Gefährdungshaftung („strict liability") handelt, ist nicht erforderlich, dass die ein *copyright* verletzende Handlung fahrlässig oder vorsätzlich begangen wurde.[370] Im Falle eines *copyright infringement* gewährt der *Copyright Act* drei Arten von Entschädigungen: Ersatz des tatsächlichen Schadens, Herausgabe des zusätzlich erzielten Verletzergewinns sowie unter bestimmten Voraussetzungen eine gesetzliche Entschädigung, die sogenannten „statutory damages".[371]

Eine wesentliche Einschränkung erfahren die dem Rechtsinhaber durch das *copyright* zugewiesenen Verwertungsrechte durch die im *common law* entwickelte sogenannte „fair use doctrine" (nachfolgend „Fair-Use-Doktrin"),[372] die unter bestimmten Voraussetzungen die Nutzung von urheberrechtlich geschützten Werken durch Dritte auch ohne Zustimmung des Rechtsinhabers in gewissen Grenzen zulässt, da in diesen, die Voraussetzungen der Fair-Use-Doktrin erfüllenden Fällen davon ausgegangen wird, dass das Allgemeinwohl („public benefit") an bestimmten freien Werknutzungen gegenüber den Interessen des Rechtsinhabers überwiegt.[373] In der Fair-Use-Doktrin kommt das dem *Copyright Act* unterliegende utilitaristische Grundprinzip zum Ausdruck, wonach das dem Rechtsinhaber durch das *copyright* zeitlich begrenzt gewährte Monopol auf die wirtschaftliche Verwertung eines Werks dem Zweck der Beförderung des allgemeinen Wohlstands der Gesellschaft verpflichtet und diesem gegebenenfalls unterzuordnen ist.[374] Die Einräumung des *copyright* verfolgt somit keinen Selbstzweck zugunsten des Rechtsinhabers, sondern dient einem ökonomischen Ziel: demjenigen, der durch die Investition von Zeit und Geld das wirtschaftliche Risiko der Erschaffung eines kreativen Produkts oder einer kreativen Leistung übernimmt, soll hierfür eine Belohnung und damit ein Anreiz zur Schaffung weiterer Werke gewährt werden. Nach Ablauf des zeitlich befristeten Monopols wird das Werk jedoch wieder ausschließlich in den Dienst des Allgemeinwohls gestellt, d.h. der Öffentlichkeit zur

369 Vgl. 17 U.S.C. § 106.
370 Vgl. *Religious Technology Center v. Netcom Online Communications* Services, 907 F. Supp. 1361, 1367 (N.D. Cal. 1995); *Kim*, 17 S. Cal. Interdis. L. J. 139, 147-48; *Patry*, in: Patry on Copyright, 2010, § 9:5, 9-19 – 9/20.
371 Vgl. 17 U.S.C. § 504(a); *Huster*, Gewinnhaftung, 2009, S. 258, 259.
372 Die Doktrin wurde zum ersten Mal in der Entscheidung *Folsom v. Marsh*, 9 F. Cas. 342 (C.C. Mass. 1841) erwähnt.
373 *Merges/Menell/Lemley*, Intellectual Property, 2003, S. 451.
374 *Merges/Menell/Lemley*, Intellectual Property, 2003, S. 325.

freien Nutzung zur Verfügung gestellt – das Werk wird Teil der „public domain".[375]

Durch die Fair-Use-Doktrin wird sichergestellt, dass auch während der Dauer des Monopols des Rechtsinhabers der Allgemeinheit ein gewisser „kreativer Freiraum" erhalten bleibt,[376] innerhalb dessen bestimmte, sozialadäquaten Zwecken dienende Handlungen, die die wirtschaftlichen Interessen des Rechtsinhabers nicht wesentlich beeinträchtigen, zulässig bleiben. Im Rahmen der Beurteilung, ob die Fair-Use-Doktrin gemäß 17 U.S.C. § 107[377] in einem konkreten Fall eingreift, müssen mehrere Faktoren berücksichtigt werden, darunter insbesondere, ob die fragliche Nutzung des Werks Auswirkungen auf dessen wirtschaftlichen (Markt-) Wert hat.

Eine weitere Einschränkung der durch das *copyright* gewährten Rechte sieht die in 17 U.S.C. § 109(a) niedergelegte sogenannte „first sale doctrine" vor, wonach der Inhaber des *copyright* keinen Einfluss darauf hat, wie derjenige, der eine rechtmäßige Kopie eines urheberrechtlich geschützten Werks auf rechtmäßigem Wege erworben hat, nach dem Erwerb mit der Kopie weiter verfährt. Der Käufer ist demnach insbesondere auch berechtigt, die Kopie an Dritte weiterzuveräußern.[378]

375 Vgl. hierzu die Entscheidung des Supreme Court in *Twentieth Century Music Corp. v. Aiken,* 422 U.S. 151, 156 (1975): *„The limited scope of the copyright holder's statutory monopoly, like the limited duration required by the Constitution, reflects a balance of competing claims upon the public interest: Creative work is to be encouraged and rewarded, but private motivation must ultimately serve the cause of promoting broad public availability of literature, music, and the other arts. The immediate effect of our copyright law is to secure a fair return to an „author's" creative labor. But the ultimate aim is, by this incentive, to stimulate artistic creativity for the general public good. ‚The sole interest of the United States and the primary object in conferring the monopoly,' this court has said, ‚lie in the general benefits derived by the public from the labors of authors.'"*; sowie in *Sony Corp. of America v. Unviersal City Studios*, 464 U.S. 417, 429 (1984): *„The monopoly privileges that Congress may authorize are neither unlimited nor primarily designed to provide a special private benefit. Rather, the limited grant is a means by which an important public purpose may be achieved. It is intended to motivate the creative activity of authors and inventors by the provision of a special reward, and to allow the public access to the products of this genius after the limited period of exclusive control has expired.".*

376 *Perritt*, 16 Mich. St. J. Int'l Law 113, 129 (2007).

377 Vgl. 17 U.S.C. § 107: *"Limitations on exclusive rights: Fair use – Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include – (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work. The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors.".*

378 *Merges/Menell/Lemley*, Intellectual Property, 2003, S. 436.

b. Deutschland

Das Gesetz über das Urheberrecht („UrhG“)[379] wurde am 13. September 1965 erlassen. Wie insbesondere aus § 11 UrhG hervorgeht, basiert es auf der Lehre der sogenannten monistischen Theorie, wonach das Urheberrecht als ein einheitliches Recht zu deuten ist, das sich sowohl aus materiellen, vermögensrechtlichen als auch ideellen, persönlichkeitsrechtlichen Elementen zusammensetzt.[380] Nach dem UrhG ist das subjektive Urheberrecht ein absolutes, „quasi-dingliches“ Ausschließlichkeitsrecht, das auf einen Gegenstand, das Werk, bezogen ist und diesen Gegenstand dem Rechtsinhaber zuordnet und seiner Herrschaft unterstellt.[381] Greift ein Dritter unbefugt in dieses Herrschaftsrecht ein, erwachsen hieraus Abwehr- und Schadensersatzansprüche gemäß §§ 97 ff. UrhG sowie ergänzend gemäß § 823 Abs. 1 BGB, da ein Urheberrecht in seiner Eigenschaft als absolutes Ausschließlichkeitsrecht auch ein sonstiges Recht im Sinne dieser Norm darstellt.

Durch den Werkbegriff werden Gegenstand und Umfang des Urheberrechtsschutzes bestimmt.[382] Das Werk ist eine „immaterielle Wesenheit“, die entweder durch unkörperliche Wiedergabe oder durch Verkörperung in einem Werkstück sinnlich wahrnehmbar wird.[383] Trotz der zentralen Bedeutung des Werkbegriffs besteht der Zweck des UrhG nicht im Schutz des Werks an sich, sondern im Schutz des Urhebers. Das Werk wird somit nur aufgrund seiner Eigenschaft als Ausdruck des individuellen schöpferischen Schaffens des Urhebers geschützt.[384] Dementsprechend wird der Begriff des Werks in § 2 Abs. 2 UrhG als „persönliche geistige Schöpfung“ definiert. Hieraus ergeben sich mehrere Elemente, die in Bezug auf das Werk vorliegen müssen, damit der Urheber hierfür Urheberrechtsschutz beanspruchen kann.[385] Es muss sich um eine persönliche Schöpfung des Urhebers handeln, die einen geistigen Gehalt aufweist und eine wahrnehmbare Formgestaltung gefunden hat, in der die Individualität des Urhebers zum Ausdruck kommt.[386] Ur-

379 Gesetz vom 09.09.1965 (BGBl. I S. 1273), zuletzt geändert durch Artikel 83 des Gesetzes v. 17.12.2008 (BGBl. I S. 2586). Das UrhG löste das Gesetz betreffend das Urheberrecht an Werken der Literatur und der Tonkunst vom 19.06.1901 ab, welches zuvor an die Stelle des Gesetzes betreffend das Urheberrecht an Schriftwerken, Abbildungen, musikalischen Kompositionen und dramatischen Werken getreten war, das der Norddeutsche Bund am 11.06.1870 erlassen hatte.

380 *Dreier/Schulze*, UrhG, 2008, § 11 Rn. 2; *Czychowski*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 11, Rn. 1.

381 *Schricker*, in: *Schricker* (Hrsg.), UrhR, 2006, Einl., Rn. 19.

382 *Schricker*, in: *Schricker* (Hrsg.), UrhR, 2006, § 2 Rn. 2.

383 *Schricker*, in: *Schricker* (Hrsg.), UrhR, 2006, Einl., Rn. 22; *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, Einl. Rn. 7 sowie § 2, Rn. 11.

384 *Schricker*, in: *Schricker* (Hrsg.), UrhR, 2006, § 2 Rn. 2.

385 *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, § 2, Rn. 7; *A. Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 2, Rn. 20.

386 *Schricker*, in: *Schricker* (Hrsg.), UrhR, 2006, § 2 Rn. 9; *Dreier/Schulze*, UrhG, 2008, § 2 Rn. 6ff; *A. Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 2, Rn. 20 ff.

heber ist gemäß § 7 UrhG derjenige, der das Werk geschaffen hat. Urheber können nach deutschem Urheberrecht nur natürliche Personen sein, nicht aber juristische Personen oder Personengesellschaften.[387]

Durch das urheberrechtliche Urheberpersönlichkeitsrecht wird die persönliche Beziehung zwischen Urheber und Werk als rechtlich selbständige Ausformung des Persönlichkeitsrechts geschützt.[388] Über die insoweit ausdrücklich getroffenen Regelungen der §§ 12-14 UrhG hinaus kommt das Urheberpersönlichkeitsrecht über den persönlichkeitsrechtlichen Kern,[389] der allen durch das Urheberrecht eingeräumten Rechtspositionen zugrunde liegt, immer dann zum Tragen, wenn dies zum Schutz der geistigen und persönlichen Interessen des Urhebers erforderlich ist.[390] Weiterhin werden durch das Urheberrecht auch die wirtschaftlichen Interessen des Urhebers geschützt, entsprechend dem in § 11 S. 2 UrhG ausdrücklich festgehaltenen Grundsatz, dass der Urheber grundsätzlich an dem wirtschaftlichen Nutzen, der aus seinem Werk gezogen wird, angemessen zu beteiligen ist. Dies geht bereits aus der Eigenschaft des Urheberrechts als Herrschaftsrecht hervor, wonach der Urheber mit seinem Werk nach freiem Belieben verfahren und es damit auch zu wirtschaftlichen Zwecken nutzen kann.[391] Darüber hinaus werden dem Urheber gemäß §§ 15 ff. UrhG jedoch spezielle Verwertungsrechte wie beispielsweise das Vervielfältigungsrecht gemäß § 16 UrhG oder das Recht der öffentlichen Zugänglichmachung gemäß § 19 a UrhG eingeräumt.[392] Weiterhin kann der Urheber Dritten an seinem Werk gemäß §§ 31, 32 UrhG bestimmte einfache oder ausschließliche Nutzungsrechte einräumen.[393] Darüber hinaus ist das Urheberrecht in seiner Gesamtheit zwar vererbbar, jedoch nicht unter Lebenden übertragbar.

Aufgrund der grundrechtlichen Sozialbindung des Eigentums, das auch für „geistiges Eigentum" gilt,[394] unterliegt das Urheberrecht bestimmten Schranken, die in §§ 44 a ff. UrhG positivgesetzlich geregelt sind.[395] Diese Schrankenbestimmungen stellen Ausnahmen von dem ansonsten gemäß § 15 UrhG geltenden Grundsatz des umfassenden Urheberrechts dar und dienen jeweils dem Schutz ei-

387 *W. Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 7, Rn. 12.
388 *Schricker*, in: *Schricker* (Hrsg.), UrhR, 2006, Vor §§ 12ff., Rn. 14; *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, Einl. Rn. 3; *Dustmann,* in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 12, Rn. 2 ff.
389 *Schulze*, in: Dreier/*Schulze*, UrhG, 2008, Vor § 12 Rn. 3.
390 *Schricker*, in: *Schricker* (Hrsg.), UrhR, 2006, Vor §§ 12ff., Rn. 8.
391 Ausprägung des Urheberrechts als „positives Nutzungsrecht", vgl. *Schricker*, in: *Schricker* (Hrsg.), UrhR, 2006, Einl., Rn. 19; *Dustmann,* in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 15, Rn. 1.
392 *Schulze,* in: *Dreier/Schulze*, UrhG, 2008, § 15 Rn. 1.
393 *Schulze,* in: *Dreier/Schulze*, UrhG, 2008, Einl. Rn. 4.
394 „Sozialbindung des Urheberrechts", vgl. *Götting*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 30, Rn. 1; *Schricker*, in: *Schricker* (Hrsg.), UrhR, 2006, Vor §§ 44 a ff., Rn. 1; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, Vor. §§ 44 a ff. Rn. 1.
395 *J.B. Nordemann„* in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, Vor §§ 44 a ff. Rn. 1.

nes spezifischen Interesses der Allgemeinheit.[396] So dient beispielsweise die Schrankenbestimmung betreffend Privatkopien gemäß § 53 UrhG dem Schutz des Interesses am privaten oder sonstigen eigenen Gebrauch von urheberrechtlich geschützten Werken. Das Zitatrecht gemäß § 51 UrhG dient dem Schutz der Freiheit des geistigen Schaffens.[397] Im Gegensatz zum US-amerikanischen Urheberrecht existiert darüber hinaus jedoch keine der Fair-Use-Doktrin vergleichbare Generalklausel, die die Nutzung urheberrechtlich geschützter Werke allgemein zu bestimmten, dem Gemeinwohl dienenden Zwecken erlauben würde. Es ist somit nach deutschem Recht nicht möglich, einen Eingriff in ein Urheberrecht beispielsweise durch den allgemeinen Verweis auf die Freiheit des Informationszugangs[398] zu rechtfertigen, wenn die Voraussetzungen keiner der gesetzlich normierten Schrankenbestimmungen erfüllt sind.

Speziell für die regelmäßig im Zusammenhang mit der Übertragung digitaler Werke über das Internet stattfindenden, urheberrechtsrelevanten Vorgänge wurde durch den Ersten Korb der Reform des Urheberrechts[399] die Schrankenbestimmung gemäß § 44 a UrhG eingeführt.[400] Durch diese Regelung werden vorübergehende Vervielfältigungshandlungen, die grundsätzlich auch von § 16 UrhG erfasst werden, unter der Voraussetzung urheberrechtlich legitimiert, dass ihnen keine „eigenständige wirtschaftliche Bedeutung" zukommt und sie „einen integralen und wesentlichen Bestandteil eines technischen Verfahrens" darstellen.[401] Weiterhin müssen solche Handlungen allein zu dem Zweck erfolgen, ein Werk innerhalb eines Netzes zwischen Dritten durch einen Vermittler zu übertragen oder eine rechtmäßige Nutzung zu ermöglichen.[402] § 44 a UrhG entzieht dem urheberrechtlichen Ausschließlichkeitsrecht somit Vervielfältigungshandlungen, die für die Übermittlung von Daten technisch erforderlich sind, die aber keine weitere wirtschaftliche Verwertung des Werks ermöglichen.[403] Dabei hatte der Gesetzgeber vor allem kurzzeitige Zwischenspeicherungen von digitalen Multimediawerken im Blick, die in Netzen, Routern oder Zwischenspeichern erfolgen oder die zur Nutzung eines urheberrechtlich geschützten Werks auf dem Computer eines Nutzers erforderlich sind, wie beispielsweise das „Routing" und „Caching".[404] Allerdings ist § 44 a UrhG insbesondere auf das „Hosting", d.h. die dauerhafte Speicherung von Infor-

396 *Schricker*, in: *Schricker* (Hrsg.), UrhR, 2006, Vor §§ 44 a ff., Rn. 4; *Götting*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 30, Rn. 1.
397 *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, Vor §§ 44 a ff. Rn. 3.
398 Vgl. hierzu *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, Einl. Rn. 25.
399 Vgl. 8. Kapitel, Teil C.I.1.b.aa.(3).
400 *Lauber/Schwipps*, GRUR 2004, 293, 295; *Schippan*, ZUM 2003, 378, 380.
401 *Götting*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010,§ 31, Rn. 206.
402 *W. Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 44 a UrhG, Rn. 4.
403 *Schippan*, ZUM 2003, 378, 380.
404 Vgl. Erwägungsgrund 33 der Multimediarichtlinie; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 44 a, Rn. 4; *Dustmann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 16, Rn. 25 a; *Loewenheim*, in: *Schricker* (Hrsg.), UrhR, 2006, § 16, Rn. 21.

mationen, nicht anwendbar, da in diesem Fall der dauerhaft gespeicherten Information durchaus eine wirtschaftliche Relevanz zukommt.[405] Insoweit ergänzt § 44 a UrhG die Haftungsbeschränkungen zugunsten von ISPs gemäß §§ 7-10 TMG, da hierdurch in Bezug auf bestimmte Tätigkeiten von ISPs, die typischerweise im Rahmen der Erbringung ihrer Dienstleistungen anfallen, die Rechte der Inhaber von Urheberrechten beschränkt werden.[406]

2. DRM-Systeme plus gesetzlicher Umgehungsschutz ist gleich Paracopyright

Sowohl im U.S.-amerikanischen *copyright law* als auch im deutschen Urheberrecht unterliegen die durch das *copyright law* bzw. das UrhG eingeräumten Rechtspositionen bestimmten Schranken. Ziel dieser Schranken ist, das Interesse des Rechtsinhabers an der Nutzung und Verwertung des Werks zu wirtschaftlichen Zwecken einerseits sowie die berechtigten Interessen der Öffentlichkeit an der Nutzung der Früchte kreativen Schaffens andererseits in Einklang zu bringen. Dieser durch das Urheberrecht geschaffene Interessenausgleich kann jedoch durch die Rechtsinhaber durch den Einsatz von DRM-Systemen einseitig außer Kraft gesetzt werden. Denn hierdurch ist es möglich, bestimmte Handlungen auf technischem Wege von vornherein auszuschließen, unabhängig davon, ob die beabsichtigte Handlung urheberrechtlich legitim ist. Denn die technische Ausgestaltung der jeweils eingesetzten DRM-Systeme, d.h. die Entscheidung darüber, welche Handlungen den Nutzern in Bezug auf das geschützte Multimediawerk erlaubt werden, können einseitig durch diejenigen festgelegt werden, die das DRM-System im Zusammenhang mit ihren Dienstleistungen einsetzen. Damit besteht jedoch die Gefahr, dass die gesetzlich vorgesehenen Schranken des Urheberrechts augehöhlt werden, da sie nur noch abstrakte Gültigkeit besitzen, jedoch von denjenigen, die davon begünstigt werden, faktisch nicht mehr genutzt werden können.

Darüber hinaus wird durch den Einsatz von DRM-Systemen das bislang geltende Prinzip in Bezug auf die Durchsetzung von Urheberrechten mit Hilfe von DRM-Systemen zulasten der Nutzer umgekehrt. War es bisher der Rechtsinhaber, der eine urheberrechtswidrige Handlung *nach* deren Eintritt beanstanden und gegebenenfalls durch Einleitung rechtlicher Schritte, einschließlich Unterlassungs-, Beseitigungs- und Schadensersatzklagen, gegen den Rechtsverletzer durchsetzen musste,[407] kann nunmehr durch DRM-Systeme eine Rechtsverletzung noch *vor*

405 *W. Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 44 a, Rn. 6; *Loewenheim*, in: *Schricker* (Hrsg.), UrhR, 2006, § 44 a, Rn. 10.

406 *Dreier/Schulze*, UrhG, 2008, § 44 a, Rn. 3. Zu §§ 7-10 TMG vgl. 8. Kapitel, Teil C.I.1.b.

407 Eine Ausnahme von diesem Rechtsschutz *ex post* stellt nur die Möglichkeit der Beantragung einer vorbeugenden einstweiligen Verfügung gemäß 17 U.S.C. § 502 bzw. § 97 Abs. 2 UrhG dar.

deren Eintritt verhindert werden. Es obliegt somit nunmehr dem Nutzer, sich gegebenenfalls gegen die Hindernisse, die ihm DRM-Systeme in Bezug auf die Ausübung einer urheberrechtlich legitimierter Handlungen in den Weg legen, zur Wehr zu setzen.[408] Diese Umkehrung in der Durchsetzung urheberrechtlicher Rechtspositionen sehen auch die Regelungen betreffend die Geltendmachung der Ausübung von Schrankenbestimmungen gemäß Art. 6 Abs. 4 Multimediarichtlinie bzw. § 95 b UrhG vor.

Dies bedeutet jedoch im Ergebnis, dass die Rechtsinhaber mit Hilfe von gesetzlich protegierten DRM-Systemen den Schutzumfang, den sie ihrem urheberrechtlich geschützten Multimediawerk gewähren wollen, nach ihren Vorstellungen selbst festlegen können („self-enforcing protection“[409] oder „Paracopyright“),[410] wodurch die insoweit geltenden urheberrechtlichen Regelungen weitgehend bedeutungslos werden.[411] Diese mit Hilfe von DRM-Systemen geschaffene *self-enforcing protection* kann zudem über die Ländergrenzen hinaus weltweit praktiziert werden, indem durch den durchgehenden Einsatz auf technischem Wege ein in allen Ländern einheitliches Schutzniveau geschaffen wird. Hingegen sind Art und Umfang des Schutzes, wie er einem Multimediawerk durch das Urheberrecht gewährt wird, von Land zu Land unterschiedlich. Denn nach den nationalen Urheberrechtsgesetzen werden dem Rechtsinhaber höchst unterschiedliche Rechtspositionen und –durchsetzungsmöglichkeiten eingeräumt abhängig von der Jurisdiktion, deren Recht nach dem Territorialitätsprinzip gerade Anwendung findet.[412]

Im US-amerikanischen Recht zeigen sich die Auswirkungen des Phänomens des durch DRM-Systeme geschaffenen Paracopyright besonders deutlich in Bezug auf die Fair-Use-Doktrin. Denn die Prüfung, ob seitens des Nutzers ein Verhalten vorliegt, dass die Faktoren der Fair-Use-Doktrin erfüllt und damit nach US-amerikanischem *copyright law* zulässig ist, erfordert eine detaillierte Einzelfallbetrachtung, die ein DRM-System regelmäßig nicht zu leisten in der Lage ist. Denn dies erfordert eine abschließende juristische Würdigung aller Umstände, die nur durch entspre-

408 *Arlt*, DRMS, 2006, S. 56; *Bechtold*, DRM, 2002, S. 279.
409 *Arlt*, s.o.; *Bechtold*, DRM, 2002, S. 280.
410 Vgl. *Nimmer*, in: Nimmer on Copyright, 2009, § 12A.18[B], 12A-186: *“Starting with the Semiconductor Chip Protection Act of 1984, continuing with the Audio Home Recording Act of 1992, and moving through the Uruguay Round Agreements Act, Congress has accreted various chapters to the Copyright Act designed to serve allied interests. Chapter 12 continues that process. It enshrines legal doctrine that “more closely resembles historic protection under the telecommunications law, or even more pointedly, the ‘Jesse James Act’ forbidding armed postal robbery, than it does the balance of Title 17”. The interests that it vindicates may therefore be dubbed “paracopyright”, as contrasted with traditional copyright protection.”.*
411 *Bechtold*, DRM, 2002, S. 370.
412 *Arlt*, DRMS, 2006, S. 56.

chend ausgebildetes menschliches Personal durchgeführt werden kann.[413] Der Umstand, dass DRM-Systeme durch die Fair-Use-Doktrin legitimierte Nutzerhandlungen als solche nicht erkennen können und damit zwangsläufig auch rechtmäßige und sozialadäquate Verhaltensweisen unterbinden, ist daher seit jeher einer der Hauptkritikpunkte der Gegner von DRM-Systemen. Dieses Argument ist von einigem Gewicht, wenn man berücksichtigt, dass in der Fair-Use-Doktrin unter anderem das im First Amendment der US-amerikanischen Verfassung niedergelegte Grundrecht auf freie Meinungsäußerung zum Ausdruck kommt.[414]

Auch nach deutschem Recht kann durch den Einsatz von DRM-Systemen ein Schutzniveau in Bezug auf Multimediawerke erzielt werden, das über den klassischen Schutzumfang, den das UrhG gewährt, in mehrfacher Hinsicht hinausgeht.[415] Wie bereits erwähnt, ist die Ausübung der Handlungen, die durch die Schrankenbestimmungen gem. §§ 44 a ff. UrhG urheberrechtlich legitimiert sind, im Zusammenhang mit DRM-Systemen erheblich erschwert. Denn der gesetzliche Schutz dieser Systeme vor Umgehung, wird auch in Bezug auf diese Schrankenbestimmungen nicht relativiert. § 95 b UrhG gewährt insoweit nur ein Anspruch des betroffenen Nutzers gegen den Rechtsinhaber auf die Zurverfügungstellung von Mitteln, die die Ausübung einer Schrankenbestimmung ermöglichen. Damit wird jedoch die Last der Durchsetzung urheberrechtlich legitimierter Handlungen auf die Nutzer übergewälzt. Zudem wird der einklagbare Rechtsanspruch gemäß

413 Die Anwendung der Fair-Use-Doktrin im konkreten Einzelfall stellt sogar die Gerichte aufgrund der Wagheit der insoweit zu berücksichtigenden Faktoren immer wieder vor Probleme, weswegen ein Richter diese Doktrin bereits als *„the most troublesome in the whole law of copyright"* bezeichnete, *Dellar v. Samuel Goldwyn, Inc.*, 1104 F.2 d 661 (2nd Cir. 1939). Der Vorwurf, dass Technologien die Fair-Use-Doktrin nicht zu berücksichtigen in der Lage sind, gilt freilich für jede Art von Technologie und damit auch für die nachfolgend im dritten Teil der vorliegenden Arbeit diskutierten Filtertechnologien, vgl. hierzu *Meyers*, 26 Cardozo Arts & Entertainment LJ 935, 951 (2009).

414 Vgl. die Ausführungen des Supreme Court hierzu in *Harper & Row, Publishers, Inc., et al. v. Nation Enterprises et al.,* 471 U.S. 539, 560 (1985): *„In view of the First Amendment protections already embodied in the Copyright Act's distinction between copyrightable expression and uncopyrightable facts and ideas, and in the latitude for scholarship and comment traditionally afforderd by fair use, we see no warrant for expanding the doctrine of fair use... ."* Diese Problematik tritt gerade auch im Zusammenhang mit den Funktionen, die den Nutzern im Rahmen von Web 2.0-Diensten (s.u. 7. Kapitel, Teil A.II, III) in Bezug auf Multimediawerke zur Verfügung gestellt werden, deutlich zutage. Dadurch wird den Nutzern die Möglichkeit eröffnet, schnell und einfach eigene Inhalte zu schaffen und diese über das Internet anderen Nutzern zugänglich zu machen. Dies hat insbesondere auch die Verbreitung sog. Mashups stark gefördert. Ein Mashup ist ein von einem Nutzer erstelltes Multimediawerk, zu dessen Herstellung der Nutzer Teile bereits existierender – gegebenenfalls urheberrechtlich geschützter –Multimediawerke verwendet hat, und der beispielsweise satirischen oder erzieherischen Zwecken dient. Mashups sind daher oftmals durch die Fair-Use-Doktrin geschützt, so dass sie ein Hauptanwendungsbeispiel für das Spannungsfeld zwischen technologischem Schutz urheberrechtlich geschützter Werke und durch die Fair-Use-Doktrin geschützte, legitime Verhaltensweisen der Nutzer darstellen.

415 *Dreyer*, in: *Pahlow/Eisfeld*, 2008, S. 221, 223.

§ 95 b UrhG nur bezüglich einiger bestimmter Schrankenbestimmungen gewährt, so dass die nicht durchsetzungsfähigen Schrankenbestimmungen im digitalen Kontext durch technische Schutzmaßnahmen faktisch ausgehebelt werden können. Dies bedeutet jedoch im Ergebnis, dass DRM-geschützte Multimediawerke vor dem Zugang der Nutzer geschützt sind, unabhängig davon, ob die vom Nutzer beabsichtigte Handlung über die bloße Umgehung der technischen Schutzmaßnahme hinaus von urheberrechtlicher Relevanz ist. Darüber hinaus können durch den Einsatz von DRM-Technologien auch Werke geschützt werden, die die gesetzlichen Voraussetzungen für den urheberrechtlichen Schutz von vornherein nicht erfüllen oder deren urheberrechtlicher Schutz wegen des Ablaufs der Schutzfrist bereits entfallen ist, da für die Anwendbarkeit des gesetzlichen Umgehungsverbots ausreicht, dass die technische Schutzmaßnahme auch, aber nicht nur, dem Schutz eines urheberrechtlich geschützten Werks dient.[416]

3. Bewertung

Durch den Einsatz von DRM-Systemen in Kombination mit den diesbezüglich eigens geschaffenen gesetzlichen Umgehungsverboten werden die Rechtsinhaber in die Lage versetzt, die Nutzung von digitalen Multimediawerken ihren eigenen Regeln zu unterwerfen und sich dabei auch über die Schranken hinwegzusetzen, die das klassische Urheberrecht zum Ausgleich der teilweise gegenläufigen Interessen der Rechtsinhaber und der Nutzer vorsieht.[417] Damit besteht die Gefahr der Schaffung eines Paracopyright, einer „private Gesetzgebung" oder eines „Überrechts"[418] außerhalb der „checks and balances" des eigentlichen Urheberrechts,[419] das den angemessenen urheberrechtlichen Interessenausgleich gefährdet.[420]

416 *Bechtold*, DRM, 2002, S. 279, 378; *Arlt*. DRMS, 2006, S. 57; *Dreyer*, in: *Pahlow/Eisfeld*, 2008, S. 221, 225.

417 *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, S. 24.

418 *Flechsig*, in: FS. *Nordemann*, 2004, S. 313, 317; *Vinje*, EIPR 1996, 431, 437; *Schulz*, GRUR 2006, 270, 276; *Bechtold*, DRM, 2002, S. 278, 279: *"DRM-Systeme bieten durch das Ineinandergreifen mehrerer Schutzmechanismen –Schutz durch Technik mit unterstützendem rechtlichem Umgehungsschutz, Schutz durch Vertrag mit unterstützendem technischem und darauf bezogenem rechtlichem Umgehungsschutz sowie Schutz durch Technologie-Lizenzverträge – neue Möglichkeiten, den Zugang zu digitalen Inhalten und deren Nutzung zu kontrollieren und unberechtigte Dritte von der Nutzung auszuschließen. Das besondere an DRM-Systemen ist das Ineinandergreifen dieser Schutzmechanismen; in ihrer Kombination schaffen sie ein Schutzniveau, das dem eines absolut wirkenden Rechts – dem Urheberrecht – ähnelt."*.

419 *Martin*, 28 Loy. L.A. Ent. L. Rev. 265, 280 (2007): : *„ ... in addition to the bundle of rights that copyright holders have always enjoyed under traditional copyright statutes, the DMCA*

Dieses durch DRM-Systeme errichtete Paracopyright schafft eine Situation, in der nicht mehr der *Copyright Act* bzw. das UrhG, sondern vielmehr die Rechtsinhaber einseitig darüber entscheiden können, welche Spielräume sie den Nutzern in Bezug auf die Nutzung eines urheberrechtlich geschützten Werks im Rahmen des jeweils eingesetzten DRM-Systems einräumen. Denn durch die Kombination technischer und gesetzlicher Mechanismen entsteht eine effektive, umfassende Zugangs- und Nutzungskontrolle zugunsten des Rechtsinhabers in Bezug auf das auf diese Weise gesicherte Multimediawerk:[421] einerseits wird durch die im Rahmen des DRM-Systems eingesetzten Technologien faktisch sichergestellt, dass nur Nutzer, deren Berechtigung, bestimmte Handlungen in Bezug auf das Multimediawerk vorzunehmen, durch das DRM-System positiv bestätigt wird, auf das Multimediawerk Zugriff erhalten; andererseits schneiden die gesetzlichen Umgehungsverbote den Nutzern die Möglichkeit der Selbsthilfe in Form der Umgehung technisch oktroyierter, zu weitgehender Einschränkungen der Nutzbarkeit des Multimediawerks ab und zwar unabhängig davon, ob der Nutzer mit der Umgehungshandlung einen urheberrechtlich legitimen Zweck verfolgt.

IV. Fehlende Akzeptanz von DRM-Systemen durch die Nutzer

> „The disparity between consumer expectations about flexible uses of digital media and limitations imposed by TPMs [technological protection measures] gives rise to significant tensions for the technology and entertainment marketplaces to mediate."[422]

Weiterhin stoßen DRM-Systeme auf überwiegende Ablehnung bei den Nutzern.[423] Die in der Literatur kaum behandelte[424] Frage der sozialen Akzeptanz von DRM-Systemen hat jedoch einen entscheidenden Einfluss auf den Erfolg dieses

expands copyright protections. By imposing liability for unauthorized circumvention of protection technologies, the DMCA creates entirely new rights and remedies pertaining to copyright infringement. The anti-circumvention provisions of the DMCA represent a significant change in American copyright tradition because it shifts the balance of competing interests away from the public to the copyright holder."

420 *Schack*, in: FS. *Schricker*, 2005, S. 511, 519.

421 *Bechtold*, DRM, 2002, S. 277.

422 *Samuelson/Schultz*, 6 J. Telecom. & High Tech. L. 41, 47 (2007.).

423 *Samuelson/Schultz*, 6 J. Telecom. & High Tech. L. 41, 42 (2007): *„Consumers of digital products ... often find TPMs* [technical protection measures] *frustrating, annoying, and harmful"*; *Fetscherin*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 305, 319; *Lehmann*, in: *Lehmann/Meents* (Hrsg.), FA IT-Recht, Kap. 10, Rn. 18; *Lehmann*, in: FS. *Pagenberg*, 2006, S. 413.

424 Lediglich *Frenzel* hat bereits im Jahr 2003 eine Arbeit betreffend die Akzeptanz von Systemen der digitalen Distribution von Musikprodukten in der Marketingforschung Arbeit verfasst, vgl. *Frenzel*, Akzeptanz im E-Commerce, 2003.

Geschäftsmodells. Denn wie bereits dargestellt wurde, hat der digitale Vertrieb von Multimediawerken bis auf weiteres einen natürlichen Konkurrenten in Form der Internetpiraterie.[425] Dies bedeutet, dass ein Nutzer gegenwärtig jederzeit die Wahl hat, ein digitales Multimediawerk anstatt über ein legales Angebot der Multimediaindustrie über eine illegale Quelle im Internet zu beziehen. Da ein in dieser Weise bezogenes digitales Multimediawerk in der Regel frei von Kosten ist sowie in seiner Nutzbarkeit keinerlei Einschränkungen durch DRM-Systeme unterworfen ist, steht die Multimediaindustrie damit vor der Herausforderung, die Nutzer davon zu überzeugen, Multimediawerke trotz der Notwendigkeit, hierfür zu zahlen und trotz der Einschränkung der Nutzbarkeit, die mit dem Einsatz von DRM-Systemen einhergehen, dennoch über das legale Angebot der Multimediaindustrie zu erwerben. Das Angebot der Multimediaindustrie muss dem Nutzer daher einen sogenannten „added value" bieten, um im Wettbewerb mit illegalen Angeboten zu bestehen.[426] Gelingt diese Überzeugungsarbeit nicht, sind auf DRM-Systemen basierende Geschäftsmodelle zum Scheitern verurteilt, da folglich die Nutzer die legalen Angebote nicht akzeptieren und anstattdessen in illegale Angebote abwandern werden.[427] Weiterhin spielt die Nutzerakzeptanz auch deswegen eine wichtige Rolle, da es im Rahmen internetbasierter Dienstleistungen in der Regel nicht um den einmaligen Verkauf eines Produkts geht, sondern um die möglichst dauerhafte Bindung der Nutzer an ein bestimmtes Dienstleistungsangebot.[428]

Um vom Nutzer als eine vorzugswürdigen Alternative gegenüber illegalen Bezugsquellen wahrgenommen zu werden, dürfen DRM-gestützte Angebote vor allem die Erwartungen, die ein Nutzer mit dessen Inanspruchnahme verbindet, nicht enttäuschen. Die Erwartungshaltung der Nutzer in Bezug auf die Nutzbarkeit von digitalen Multimediawerken und den damit im Zusammenhang stehenden Dienstleistungen und Produkten ist vor allem durch die Erfahrungen aus der Vergangenheit beim Umgang mit traditionellen analogen Medien geprägt.[429] Dazu gehört insbesondere die Möglichkeit, von einem rechtmäßig erworbenen Multimediawerk Kopien erstellen zu können, entweder zu dem Zweck, um sich damit vor dem Verlust oder der Beschädigung des Originals zu schützen, oder aber, um das Multimediawerk auch über andere Endgeräte konsumieren zu können.[430] Auch besteht insbesondere im Filmbereich seit Einführung des Videorekorders seitens der Nutzer ein Interesse daran, einmal öffentlich übertragene Filmwerke aufzuzeichnen

425 Vgl. 3. Kapitel, Teil B.I sowie 5. Kapitel, Teil B.I.
426 *Rump*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 3, 5.
427 *Biddle/England/Peinado/Willman*, The Darknet and the Future of Content Distribution, S. 1, 11, abrufbar unter http://msl1.mit.edu/ESD10/docs/darknet5.pdf (zuletzt abgerufen am 01.07.2010).
428 *Frenzel*, Akzeptanz im E-Commerce, 2003, S. 94.
429 *Samuelson/Schultz*, 6 J. Telecom. & High Tech. L. 41, 44 (2007).
430 *Samuelson/Schultz*, s.o.

und zu einem späteren Zeitpunkt zu konsumieren (sogenanntes „time-shifting"). Dieses Interesse am *time shifting*, dessen rechtliche Zulässigkeit im US-amerikanischen *copyright law* als rechtlich legitim anerkannt ist,[431] hat sich in der Zwischenzeit auch auf andere Bereiche übertragen, indem Nutzer beispielsweise auch Radiosendungen zum Zeitpunkt ihrer Wahl anhören wollen und zu diesem Zweck solche Sendungen in Form von Podcasts im Internet abrufen und herunterladen und nach Belieben abspielen können wollen. Da die Nutzer daher bereits aus der Vergangenheit in gewissem Umfang daran gewöhnt sind, zu vielfältigen Zwecken Kopien von Multimediawerken erstellen zu können, erwarten sie, dass ihnen diese Möglichkeit auch im Zeitalter der Digitalisierung offen steht: Zusätzlich erwarten sie jedoch, von der Flexibilität, die mit der Digitalisierung von Inhalten einhergeht, zu profitieren.[432] Konkret bedeutet dies, dass die Nutzer ein rechtmäßig erworbenes digitales Multimediawerk jederzeit, über jegliche digitale Endgeräte und überall, d.h. sowohl zuhause, in der Familie und bei der Arbeit konsumieren sowie in gewissem Umfang diesen Konsum mit anderen teilen und von dem Multimediawerk Kopien für nicht-kommerzielle Zwecke anfertigen können wollen.[433]

Zu dieser Erwartungshaltung gesellt sich eine sehr niedrige Toleranzschwelle der Nutzer in Bezug auf technologische Beschränkungen der Nutzbarkeit von digitalen Inhalten.[434] Beschränkungen der Möglichkeit, Inhalte zu vervielfältigen und an Dritte zu übermitteln sowie der Zwang, vor der Nutzung eines Inhalts eine bestimmte Software herunterladen oder sich registrieren zu müssen, werden überwiegend abgelehnt.[435] Noch unbeliebter sind Beschränkungen der Interoperabilität zwischen Inhalten und digitalen Endgeräten, die zeitliche Begrenzung der Nutzbarkeit von Inhalten sowie die Überwachung und Nachverfolgung der Handlungen der Nutzer durch DRM-Systeme.[436] Dies bedeutet im Umkehrschluss, dass der Nutzer vor allem an einem Angebot zum Konsum digitaler Inhalte interessiert ist, durch das ihm flexible Verwendungsmöglichkeiten eingeräumt werden, die dauerhafte Nutzbarkeit des Inhalts sichergestellt ist und zudem sein Interesse an der

431 Vgl. *Sony Corp. of America v. Universal City Studios,*, 464 U.S. 417 (1984).

432 *Samuelson/Schultz*, 6 J. Telecom. & High Tech. L. 41, 45 (2007): „*Consumers may, for example, expect to be able to link works together, format-shift, annotate them, tinker with them, remix and mashup existing digital content, and share their new creations with others"*; vgl. auch den Bericht des INDICARE-Projekts von *Helberger* (Hrsg.), DRM and Consumer Acceptability, 2005, S. 3-5, abrufbar unter http://www.indicare.org/tiki-download_file.php?fileId=111 (zuletzt abgerufen am 01.07.2010) worin die von den Nutzern gewünschte neue Flexibilität bei der Nutzung digitalisierter Inhalte unter dem Stichwort "Authorized Domain" beschrieben wird.

433 *CDT*, Evaluating DRM, 2006, S. 14; vgl. auch *Lincoff*, 2 J. Int'l Media & Ent. L. 1, 27 (2008-2009): *„People develop an ownership interest in the music they most like to hear."*

434 *Fetscherin*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 305, 315.

435 *Fetscherin*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 305, 316.

436 *Fetscherin*, s.o.

Respektierung der Privatsphäre und der Vertraulichkeit seiner persönlichen Daten angemessen berücksichtigt wird.

DRM-gestützte Geschäftsmodelle stehen daher vor einer zweifachen Herausforderung: zum einen müssen sie der aufgezeigten Erwartungshaltung der Nutzer möglichst gerecht werden; zum anderen müssen sie die bereits bestehenden Vorbehalte der Nutzer gegenüber dem Einsatz von DRM-Systemen begegnen und abbauen. Diese Herausforderungen haben DRM-Systeme jedoch bisher noch nicht gemeistert,[437] worin einer der hauptsächlichen Gründe für ihr Scheitern im Zusammenhang mit Musikdownloads liegt. Denn die aufgezeigten Nachteile der mittlerweile aufgegebenen DRM-Systeme im Bereich der Musikdownloads[438] stellen gleichzeitig die größten Hindernisse für die Akzeptanz solcher Systeme durch die Nutzer dar: mangelnde Interoperabilität, fehlende Nachhaltigkeit und Beeinträchtigung des Daten- und Verbraucherschutzes. Die Multimediaindustrie muss sich daher vorwerfen lassen, dass sie es versäumt hat, DRM-Systeme so zu gestalten, dass die dagegen seitens der Nutzer bestehenden begründeten Vorbehalte entkräftet wurden.[439] Denn bisher wurden DRM-Systeme vor allem auf einen möglichst umfassenden Schutz für digitale Multimediawerke ausgerichtet und darüber die technische Akkommodierung legitimer, durch die Urheberrechtsgesetze ausdrücklich zugelassener Handlungen der Nutzer weitgehend vernachlässigt.[440] Infolgedessen steht jedoch aus Sicht der Nutzer beim Einsatz von DRM-Systemen nicht der Schutz der sich aus dem Urheberrecht ergebenden, berechtigten Interessen der Rechtsinhaber, sondern vielmehr die Erosion der ebenfalls durch das Urheberrecht garantierten Rechte der Nutzer im Vordergrund. Dieser Umstand und die daraus folgende Ablehnung DRM-gestützter Angebote verhindert jedoch, dass sich die Angebote aus Sicht der Nutzer langfristig als echte Alternativen gegenüber illegalen Angeboten etablieren können.

C. Neue Geschäftsmodelle der Musikindustrie nach dem Scheitern des DRM-gestützten Download-Vertriebs

> „Music and technology share a long, intimate history. Technology is the magic that allows us to capture the ephemeral and elusive experience of music in a form that may be shared with others. … New technologies, and those that create

437 *CDT*, Evaluating DRM, 2006, S. 17: *„As much as possible, DRM solutions should seek to allow users to interact with, excerpt, and expand on existing works in ways that are consistent with copyright law. ... DRM is currently not well adapted to the task of facilitating end user creation"*.

438 Vgl. 5. Kapitel, Teil B.II.

439 *Rump*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 3, 5.

440 *Fetscherin*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 305, 315.

them, affect how music is made, shared and sold. That impact has economic and legal implications. It has encouraged new entrants, created new markets, and made possible new products. It has also forced established businesses to react and to reconsider both how they do business and what their business really is."[441]

Der Verzicht auf DRM-Systeme beim Vertrieb von Musikdownloads ist Ausdruck des grundsätzlichen Umdenkens, das derzeit in der Musikindustrie stattfindet. Dabei wird das Internet nicht länger als ein notwendiges Übel und als Gefahr für die tradierten Geschäftsmodelle, sondern als Chance für neue Vertriebs- und Vermarktungswege begriffen.

I. Paradigmenwechsel in der Tonträgerindustrie

„The impetus to lift copyright protection represents a sea change for the recording industry, which for the better part of a decade has used DRM to guard against what it considers illegal distribution and duplication of songs purchased online."[442]

Der Verzicht auf DRM-Systeme beim Vertrieb von Musikdownloads, der bis vor kurzem noch undenkbar erschien,[443] stellt einen Versuch der Musikindustrie dar, auf die durch die Digitalisierung veränderte Nachfrage der Kunden sowie die neuen Marktrealitäten zu reagieren.[444] Dabei verabschieden sich vor allem die Tonträgerunternehmen zunehmend von der Vorstellung, die Kontrolle über den Vertrieb von digitalen Tonaufnahmen mit Hilfe von DRM-Systemen vollständig wiederherzustellen und dadurch ihr tradiertes Geschäftsmodell in das Zeitalter der Digi-

441 *Krasilovsky/Shemel*, Music Business, 2007, S. 414.

442 *Holahan*, Sony BMG Plans to Drop DRM, businessweek.com, 04.01.2008, http://www.businessweek.com/print/technology/content/jan2008/tc2008013_389775.htm (zuletzt abgerufen am 01.07.2010).

443 Vgl. beispielsweise folgende Stellungnahme zum Thema DRM von *Nora Braun*, Justiziarin der Deutschen Phonoverbände, auf der 6. Fachtagung in der Reihe „Allianz von Technik und Recht" am 4. und 5. Mai 2006 in Stuttgart: *„Für die Musikwirtschaft ist die technische Entwicklung von DRM-Systemen von erheblicher Bedeutung. Sie ist unverzichtbar, um Musikplattformen im Online-Bereich und den Vertrieb von Musik im Mobile-Entertainment-Bereich weiter auf dem Markt zu etablieren und so dem Verbraucher jenseits physischer Formate eine neue Form von legalem Musikgenuss zu ermöglichen"*; *Braun*, in: *Roßnagel*, Digitale Rechteverwaltung, 2009, S. 53.

444 Einhorn, 56 J. Copyright Soc'y 201 (2008).

talisierung zu übertragen,[445] zugunsten eines neuen Ansatzes, nach dem die existierenden Vertriebs- und Vermarktungsstrategien an die durch die Digitalisierung und die zunehmende Verbreitung des Internets geschaffenen neuen Verhältnisse anzupassen sind.

Dieser neue Ansatz wird durch eine Vielzahl von Äußerungen seitens der Entscheidungsträger der Tonträgerindustrie belegt. So gibt beispielsweise Universal mittlerweile unumwunden zu, dass weder der Einsatz von DRM-Systemen noch Klagen gegen einzelne Nutzer von illegalen Filesharing-Netzwerken eine ausreichende Reaktion auf die Herausforderungen, vor die das Internet die Musikindustrie stellt, darstellen, sondern vielmehr die Geschäftsmodelle in ihrer bestehenden Form grundsätzlich hinterfragt und dabei die Erwartungen des Marktes in Form der Nutzer, der Händler und der Künstler angemessen berücksichtigt werden müssen.[446] Dementsprechend sei der Verzicht auf DRM-Systeme im Downloadbereich eine erste Reaktion auf die Signale des Marktes, ebenso wie die Entscheidung im Bereich von Streaming-Angeboten von kostenpflichtigen Abonnementmodellen auf einen für die Nutzer kostenfreien, werbebasierten Ansatz umzustellen. Da die Musikindustrie weiterhin zunehmend anerkenne, dass nicht mehr jeder Nutzer am käuflichen Erwerb von digitalen Tonaufnahmen interessiert sei, bemühe man sich darum, vor diesem Hintergrund neue Geschäftsmodelle zu entwickeln. Dabei dürften die Umsätze der Tonträgerindustrie nicht mehr in erster Linie von dem Verkauf einzelner Musiktitel und -alben abhängen, sondern müssten mehr an den einzelnen Nutzer sowie die von ihm zum Konsum von Musik bevorzugten Kanäle gekoppelt werden.[447] Der Schlüssel zur Lösung des derzeitigen Dilemmas liege somit in der Schaffung neuer Geschäftsmodelle und der Diversifikation von Einnahmequellen unter Berücksichtigung der Wünsche der Nutzer nach Interoperabilität.[448] Das Ziel müsse sein, der breiten Masse der Nutzer Musikangebote zu jeder Zeit und an jedem Ort so einfach wie möglich zugänglich zu machen, um dadurch illegalen Angeboten die Existenzgrundlage zu entziehen.[449]

445 *Rick Rubin*, Chef des zu Sony Music Entertainment gehörigen Plattenlabels Columbia Records, geht davon aus, dass das auf dem Direktverkauf von physischen Tonträgern basierende Geschäftsmodell „erledigt" ist, vgl. *Hirschberg*, The Music Man, 02.09.2007, The New York Times, http://www.nytimes.com/2007/09/02/magazine/02rubin.t.html?pagewanted=5&_r=1&ei=5087&em&en=314fd873126f1af6&ex=1189051200 (zuletzt abgerufen am 01.07.2010).

446 Im Interview mit CNET, vgl. *Sandoval*, Universal digital chief on iTunes, DRM, and Android, CNET News, 12.01.2009, http://news.cnet.com/8301-1023_3-10140244-93.html?part=rss&tag=feed&subj=News-DigitalMedia (zuletzt abgerufen am 01.07.2010).

447 Vgl. *Sandoval*, s.o.

448 Vgl. *Sandoval*, s.o.

449 Vgl. *Sandoval*, s.o.; die Zahlen scheinen die strategische Neuausrichtung des Konzerns zu bestätigen, wonach in den ersten drei Quartalen des Jahres 2008 der Umsatz insgesamt um 3,5 Prozent auf fast US$ 4 Mrd. angestiegen war, wozu ein Wachstum des Erlöses aus digitalen Verkäufen um 33 Prozent beigetragen hatte.

In ähnlicher Weise äußerten sich auch Warner und Sony.[450] Die bislang eingesetzten DRM-Systeme seien hinter den Erwartungen der Tonträgerunternehmen zurückgeblieben. Man müsse daher den Wunsch der Nutzer, sich mit anderen über Musik austauschen zu können, als neue Realität anerkennen und Wege finden, diese Aktivitäten der Nutzer zu kanalisieren und zu unterstützten, um auf diese Weise davon zu profitieren.

Auch zeigen Studien, dass die Nachfrage nach Musik in den USA weiterhin ungebrochen ist und in den letzten fünf Jahren sogar noch erheblich angestiegen ist.[451] So geht aus dem Digital Music Report 2009 der International Federation of the Phonographic Industry („IFPI") hervor, dass das Gesamtvolumen konsumierter Musik zwischen 2003 und 2007 um ein Drittel angestiegen ist. Ein Grund dafür ist die zunehmende Verbreitung portabler digitaler Endgeräte, durch die die Nutzer in die Lage versetzt werden, ihre gesamte Musik überall mit hinzunehmen und sie zu jeder Zeit und an jedem Ort zu hören, was den Zeitraum, währenddessen theoretisch an jedem Tag Musik konsumiert werden kann, verlängert.[452] Dementsprechend verzeichnete der Informationsdienst Nielsen SoundScan für den US-amerikanischen Markt einen Anstieg in der Anzahl getätigter Transaktionen im Zusammenhang mit Musikprodukten quer durch alle derzeit verfügbaren Vertriebswege und Formate gegenüber dem Vorjahr um 10,5 Prozent.[453]

II. Diversifikation der Vertriebswege

> „An incredible revolution is sweeping the music industry ... . In the US ... 30 per cent of all recorded music sold is online or mobile. Record labels are becoming broad-based entertainment companies, developing new revenue streams. The consumer has better choice, availability and flexibility in enjoying music than ever before.
> Our digital revenues are growing and diversifying as our business model changes from one dominant format to hundreds of channels and products."[454]

Die neue Strategie der Tonträgerunternehmen besteht somit darin, sich möglichst viele neue Vertriebswege als neue Einkommensquellen zu erschließen. Dabei

450 *Shinal*, Warner Music's Bronfman on DRM-free tunes. The technology never did what it needed to do, vatornews, 07.11.2008, http://vator.tv/news/show/2008-11-07-warner-musics-bronfman-on-drm-free-tunes (zuletzt abgerufen am 01.07.2010); *Hirschberg*, The Music Man, 02.09.2007, The New York Times, http://www.nytimes.com/2007/09/02/magazine/02rubin.t.html?pagewanted=5&_r=1&ei=5087&em&en=314fd873126f1af6&ex=1189051200 (zuletzt abgerufen am 01.07.2010).
451 *IFPI*, Digital Music Report 2008, S. 4.
452 *Perritt*, 16 Mich. St. J. Int'l Law 113, 117 (2007.).
453 *IFPI*, Digital Music Report 2009, S. 4.
454 Vgl. *IFPI*, Digital Music Report 2008, S. 3.

zeichnet sich ein Trend ab weg von der bisherigen vollumfänglich proprietären Distribution, d.h. dem Vertrieb von digitalen Tonaufnahmen unter dem Vorbehalt aller Rechte und der aktiven Durchsetzung der Einhaltung der Nutzungsbedingungen durch DRM-Systeme, hin zu offeneren Geschäftsmodellen, wonach digitale Tonaufnahmen möglichst umfassend über vielfältige Plattformen und digitale Endgeräte verfügbar gemacht werden, und die oftmals auf der Verbindung von frei verfügbaren digitalen Inhalten mit Werbung basieren.[455]

1. Erhöhung der Attraktivität von Onlineshops

Onlineshops, über die Nutzer Musikdownloads käuflich erwerben können, sind für die Nutzer bereits aufgrund der Aufgabe des Einsatzes von DRM-Systemen wesentlich attraktiver geworden. Denn die nunmehr überwiegend im MP3-Format vertriebenen Musikdownloads kann man problemlos auf fast allen digitalen Endgeräten abspielen, insbesondere auch auf dem weitverbreiteten iPod von Apple.[456] Allerdings vertreibt gerade der Anbieter Apple Musikdownloads über seinen iTunes-Store noch immer nicht im MP3-, sondern im qualitativ hochwertigeren AAC-Format,[457] das nicht von allen MP3-Playern unterstützt wird und insoweit die Flexibilität der Nutzer weiterhin etwas beschränkt.[458] Dessen ungeachtet hat sich das MP3-Format faktisch als Standardformat im Bereich von Musikdownloads etabliert.[459]

2. Vorantreiben der Etablierung von Subscription Services

Weiterhin werden sogenannte „subscription services" wie beispielsweise Napster 2.0 oder Rhapsody angeboten, d.h. Abonnementangebote, in deren Rahmen die Nutzer gegen Zahlung einer monatlichen Gebühr während der Dauer des Abon-

455 *Montagnani*, 26 Cardozo Arts & Ent. L.J. 719, 770 (2009).

456 *Hansen*, Gesprengte Ketten – Legale MP3-Downloads in Deutschland, c't 2009, Heft 9, S. 137.

457 AAC steht als Abkürzung für „Advanced Audio Coding" und ist ein Format zur verlustbehafteten Audiokomprimierung, das mit dem MP3-Format konkurriert.

458 *Hansen*, Gesprengte Ketten – Legale MP3-Downloads in Deutschland, c't 2009, Heft 9, S. 138.

459 *Hansen*, Gesprengte Ketten – Legale MP3-Downloads in Deutschland, c't 2009, Heft 9, S. 137; für die Anbieter der Downloaddienste allerdings bedeutet der MP3-Vertrieb zunächst höhere Kosten, da zum einen das auszuliefernde Datenvolumen steigt, da MP3 gegenüber den bisher vertriebenen Dateiformaten wie beispielsweise WMAeine höhere Bitrate von 320 kBit/s verzeichnet. Darüber hinaus fallen bei einer Lieferung von Musikdateien im MP3-Format im Gegensatz zu WMA oder AAC zusätzliche Lizenzgebühren in Höhe von zwei Prozent Umsatzbeteiligung zugunsten der MP3-Rechteinhaber an.

nements Zugang zu dem gesamten Musikkatalog des Anbieters erhalten. Im Unterschied zu Onlineshops können die Nutzer von *subscription services* die Tonaufnahmen nicht dauerhaft auf ihren Computer herunterladen. Vielmehr wird die gewünschte Datei auf ihren Computern in Form eines Streams[460] wiedergegeben.

Allerdings leidet das Angebot der *subscription services* darunter, dass deren Musikkataloge zumeist wesentlich beschränkter sind als diejenigen von Onlineshops, was ein erhebliches Hindernis für das Wachstum dieses Geschäftsmodells darstellt.[461] Weiterhin sind in der Regel die Nutzungsmöglichkeiten des im Rahmen des *subscription services* verfügbaren Musikrepertoires begrenzt, indem die Übertragung der Musikdateien vom Computer des Nutzers auf andere digitale Endgeräte oder die Erlaubnis zu deren Nutzung über den Abonnementzeitraum hinaus – wenn überhaupt – nur gegen Zahlung einer zusätzlichen Gebühr möglich ist.[462] Dem Erfolg von *subscription services* stehen somit derzeit noch Nachteile der Nutzer in Bezug auf die Interoperabilität und die Nachhaltigkeit der über diese Dienste nutzbaren Inhalte im Weg.[463] Dementsprechend spielen im Rahmen dieser Dienste DRM-Systeme weiterhin eine wichtige Rolle, etwa bei der Verifizierung der Berechtigung des Nutzers betreffend die Nutzung des Dienstes.

Weiterhin haben *subscription services* den Nachteil, dass die Nutzer die Musikdateien in der Regel nicht dauerhaft zu Eigentum erwerben und auf ihren Computern speichern, sondern nur während der Dauer des Abonnements abrufen können. Aufgrund der zeitlich begrenzten Verfügbarkeit der Musikdateien sind diese Angebote jedoch insbesondere für jüngere Nutzer weniger attraktiv als Onlineshops. Denn gerade diese Nutzergruppe entwickelt in Bezug auf ihre favorisierte Musik naturgemäß ein starkes „Eigentümerinteresse“,[464] d.h. ein Interesse an einer

460 Vgl. 4. Kapitel, Teil B.III.2.

461 Dass die Anbieter von *subscription services* im Rahmen ihrer Dienste weniger Musiktitel anbieten können, liegt darin begründet, dass zum Betrieb eines solchen Dienstes zusätzlich zu der Berechtigung, die urheberrechtlich geschützte Tonaufnahme im Rahmen des Dienstes temporär vervielfältigen und verbreiten zu dürfen, zusätzlich die Erlaubnis zur Nutzung des der jeweiligen Tonaufnahme unterliegenden Musikwerks benötigen. Denn der Copyright Act sieht nur für die *„digital phonorecord delivery“*, d.h. die dauerhafte „Lieferung“ einer digitalisierten Tonaufnahme beispielsweise in Form eines Downloads, nicht aber für deren lediglich temporäre Wiedergabe eine Zwangslizenz *(„compulsory license“)* in Bezug auf das der Tonaufnahme unterliegende Musikwerk vor. Daher müssen die Anbieter von *subscription services* in Bezug auf jede Tonaufnahme, die sie in ihren Musikkatalog aufnehmen und auf den Computern der Nutzer lediglich temporär in Form eines Streams wiedergeben wollen, zusätzlich die Rechte an dem der Tonaufnahme unterliegenden Musikwerk einholen. Vgl. zu dieser Problematik *Einhorn*, Gorillas in Our Midst, 2007, S. 11, sowie *Lincoff*, 2 J. Int’l Media & Ent. L. 1, 17 ff. (2008-2009).

462 *Montagnani*, 26 Cardozo Arts & Ent. L.J. 719, 759 (2009).

463 *Einhorn*, 56 J. Copyright Soc’y, 201, 204 (2008).

464 *Lincoff*, 2 J. Int’l Media & Ent. L. 1, 27 (2008-2009): *„People develop an ownership interest in the music they most like to hear.“*.

möglichst uneingeschränkten Verfügungsmacht hierüber.[465] Dies belegt eine im Sommer 2009 im Auftrag des Dachverbandes der britischen Musikindustrie UK Music durchgeführte Studie, aus der hervorgeht, dass Nutzer im Alter zwischen 14 und 24 viel Wert darauf legen, dass die Nutzbarkeit ihrer Musik auf Dauer sichergestellt ist.[466] Deswegen erfreuen sich Onlineshops in dieser Altersgruppe einer höheren Beliebtheit als Abonnementdienste, da der Zugang zu auf einen Computer oder ein portables digitales Endgerät heruntergeladenen Musikdateien anders als bei Streaming-Angeboten[467] zu jeder Zeit gewährleistet ist.[468] Aus demselben Grund erfreut sich auch das Trägermedium CD weiterhin einer großen Beliebtheit in dieser Altersgruppe.

Daraus kann geschlossen werden, dass wohl nur ein Modell, das gerade jüngeren Nutzern die Möglichkeit bietet, zu einem erschwinglichen Preis eine große Anzahl an dauerhaft verfügbaren Musik-Downloads zu erwerben, in dieser Altersgruppe ein wirksames Gegenmittel gegen Internetpiraterie bieten wird. Ausweislich der Studie von UK Music erklärten 85 Prozent der Befragten, dass sie bereit wären, für eine solche Dienstleistung, die dauerhaften Zugang zu Musikdateien gewährt, zu zahlen und über die Hälfte erklärte sich sogar bereit, in diesem Fall von der Nutzung illegaler Tauschbörsen abzusehen. Bisher gibt es jedoch nur wenige, vereinzelte Ansätze seitens der Musikindustrie, Musikangebote auf die speziellen Bedürfnisse des jüngeren Publikums zuzuschneiden. Eines dieser wenigen Beispiele ist das von dem Unternehmen Warner Music im Sommer 2008 initiierte „Choruss-Programm" für US-amerikanische College Studenten.[469]

465 Auch ähnelt der Kauf einer Tonaufnahme in Form eines Downloads am meisten dem traditionellen Erwerb eines phyischen Datenträgers. Aus diesem Grund entschied sich beispielsweise Apple dafür, im Rahmen seines iTunes-Store ausschließlich Downloads anzubieten, weil man davon ausging, dass die Nutzer dieses Produkt einem Streaming-Angebot vorziehen würden, vgl. *Krasilovsky/Shemel*, Music Business, 2007, S. 429.

466 Die Ergebnisse der Studie, die von *Bahanovic/Callopy* von der Music and Entertainment Industries Research Group der University of Hertforshire 2009 durchgeführt wurde, ist abrufbar unter http://www.ukmusic.org/files/UK%20Music_Uni%20Of%20Herts_09.pdf (zuletzt abgerufen am 01.07.2010).

467 Vgl. 4. Kapitel, B.III.2.

468 Vgl. *Krasilovsky/Shemel*, Music Business, 2007, S. 429: *"Subscription models offer access to music at lower cost measured in the short term, but at a higher price over the long term, and with the constant threat that access will be cut off if the subscription is not continued. Properly conveying this understanding to individuals is more complicated"*.

469 *Heise Online*, US-Musikindustrie experimentiert mit P2P-Flatrate für Studenten, 10.12.2008, http://www.heise.de/newsticker/meldung/120220 (zuletzt abgerufen am 01.07.2010).

Ein weiteres Modell, in dem die Musikindustrie großes Potential für zukünftiges Wachstum sieht, ist die Kommerzialisierung des mobilen Zugangs zu Musik, d.h. die Verbindung von Musikangeboten mit portablen digitalen Endgeräten. Dieses Geschäftsmodell setzt auf die zunehmende „digitale Konnektivität" der Nutzer, d.h. die Integration von digitalen Netzwerken mit Computern sowie mit Notebooks, Mobiltelefonen, MP3-Playern, Smartphones[470] und anderen digitalen Endgeräten.[471] Ein Beispiel hierfür ist die Verbindung von Mobilfunkverträgen mit einer Musikflatrate, wie beispielsweise das im Jahr 2008 angelaufene „Comes With Music"-Angebot von Nokia, dem finnischen Hersteller von Mobiltelefonen.[472] Die Kosten für solche Geschäftsmodelle können durch Preisaufschläge beim Verkauf der jeweiligen Geräte bzw. durch Erhöhung der vertraglichen Gebühr für die Gewährung des Zugangs zu einem Netzwerk, in dessen Rahmen die entsprechenden Musikangebote genutzt werden können, gedeckt werden.[473] Damit gewinnt die Kooperation mit Technologieunternehmen und Netzwerkbetreibern für die Musikindustrie zunehmend an Bedeutung.[474]

Auch im Bereich dieses sogenannten „mobile commerce" („M-Commerce") wird, soweit hierüber Musikdownloads vertrieben werden, zunehmend auf den Einsatz von DRM-Systemen verzichtet.[475] Dieser Umstand ist von nicht zu unterschätzender Bedeutung, da der Markt für den Vertrieb von digitalen Tonaufnahmen über portable digitale Endgeräte als einer der größten Wachstumsmärkte für den zukünftigen Vertrieb von Musik gilt, der für die umsatzstärksten Künstler aus den

470 Mobiltelefone, die mit sog. PIM-Software zum Lesen und Schreiben von Emails ausgerüstet sind wie beispielsweise der Blackberry der Firma RIM (Research in Motion) oder das iPhone von Apple.

471 So lautet das Motto des jährlichen der IFPI für das Jahr 2010 auch *„Music how, when, where you want it"*, vgl. *IFPI*, Digital Music Report 2010; vgl. auch *Dong Ngo*, Internet usage via handheld devices soars, CNET News, 18.08.2009, http://news.cnet.com/8301-1035_3-10312296-94.html (zuletzt abgerufen am 01.07.2010).

472 *IFPI*, Digital Music Report 2009, S. 4; Musikindustrie setzt auf Kombi-Angebote und „Three Strikes", heise online, 17.9.2009, http://www.heise.de/newsticker/meldung/125474 (abgerufen am 23.9.2009)..

473 *Bonstein*, Kundensuche im Feindesland, Der Spiegel, 16/2009, S. 100, 101.

474 Vgl. hierzu *Reinke*, Wertschöpfungsmöglichkeiten Musikindustrie, 2009, S. 28 ff.; *Clement/Schusser/Papies*, in: *Clement/Schusser/Papies*, Ökonomie Musikindustrie, 2008, S. 6; *Krasilovsky/Shemel*, Music Business, 2007, S. 415.

475 So verkündete die Telekomtochter T-Mobile im Jahr 2009, die im Rahmen ihres Onlineshops Jukebox vertriebenen Musikdownloads auf Grundlage einer Vereinbarung mit allen großen Tonträgerunternehmen ohne Kopierschutz zu vertreiben, vgl. *Greif*, T-Mobile Jukebox verzichtet auf DRM, ZDNET.de, 05.06.2009, www.zdnet.de/news/lebensart_lifestyle_digital_t_mobile_jukebox_verzichtet_auf_drm_story-39001025-41004968-1.htm (zuletzt abgerufen am 01.07.2010); *c't news*, T-Mobile bietet kopierschutzfreie Musik-Downloads an, 07.06.2009, www.heise.de/ct/T-Mobile-bietet-kopierschutzfreie-Musik-Downloads-an---/news/meldung/140000 (zuletzt abgerufen am 01.07.2010).

Musikbereichen Pop oder R&B bereits 20 bis 45 Prozent ihrer Umsätze ausmacht.[476]

4. Expansion in weitere branchennahe Geschäftsfelder: Stichwort „360°-Modell"

Weiteres großes Potential bietet der Vertrieb von Produkten im Zusammenhang mit bekannten Künstlern und deren Musik („Merchandising"),[477] beispielsweise die Lizenzierung von populären Musiktiteln für Computerspiele. So wurde das Computerspiel „Guitar Hero" des kalifornischen Unternehmens Activision seit 2006 mehr als 20 Millionen Mal verkauft.[478] Auch die Konzertvermarktung stellt ein sehr lukratives Marktsegment dar. Bestes Beispiel hierfür ist das Unternehmen Live Nation, das sich innerhalb kurzer Zeit als der weltweit größte Konzertvermarkter etabliert hat und der Stars wie Madonna, The Rolling Stones, U2 und Coldplay unter Vertrag hat.[479] Diese Künstler bindet das Unternehmen in sogenannten 360°-Verträgen umfassend an sich, wobei die Künstler neben den Rechten zur Vermarktung von Konzerten auch sämtliche Rechte betreffend die Herstellung und den Vertrieb von Tonaufnahmen und damit verbundenen Merchandisingprodukten an das Unternehmen übertragen. Das Unternehmen übernimmt somit das Management dieser Künstler für sämtliche Bereiche, die wirtschaftlich von Bedeutung sind.[480]

Vor dem Hintergrund dieser Entwicklungen haben auch die Tonträgerunternehmen erkannt, das sie sich zukünftig verstärkt in allen Bereichen der Wertschöpfung betätigen müssen, d.h. neben den traditionellen Bereichen im Zusammenhang mit dem Vertrieb von Tonaufnahmen auch in den Bereichen Künstlermanagement, Konzerte und Ticketing sowie weiteren branchennahen Geschäftsfeldern.[481]

476 *Sandoval*, UMG digital chief on iTunes, DRM, and Android, CNET News, 12.01.2009, http://news.cnet.com/8301-1023_3-10140244-93.html?part=rss&tag=feed&subj=News-DigitalMedia (zuletzt abgerufen am 01.07.2010).
477 *Theurer*, Geldregen auf der Bühne, FAZ.NET, 19.09.2007, http://www.faz.net/s/Rub-D16E1F55D21144C4AE3F9DDF52B6E1D9/Doc~E48F4D01A669D48E1A27ACD3A9C87B3CD~ATpl~Ecommon~Scontent.html (zuletzt abgerufen am 01.07.2010).
478 *Theurer*, Auf der Suche nach der Zukunft, Frankfurter Allgemeine Zeitung, 09.04.2009, S. 21; *Einhorn*, 56 J. Copyright Soc'y, 201, 207 (2008).
479 *Einhorn,* Gorillas in Our Midst, 2007, S. 14-15.
480 *Ingendaay*, DAJV Newsletter 2009, S. 108, 111.
481 *Reinke*, Wertschöpfungsmöglichkeiten Musikindustrie, 2009, S. 18, 63 ff..

III. Zahlen und Fakten zur aktuellen Entwicklung des digitalen Sektors des US-amerikanischen und deutschen Musikmarkts

1. USA

Der Anteil digitaler Musikverkäufe an den in den USA im Jahr 2009 mit dem Vertrieb von Tonaufnahmen insgesamt erzielten Einnahmen stieg im Jahr 2009 auf 41 Prozent,[482] gegenüber 34 Prozent im Vorjahr. Der im digitalen Marktsegment erzielte Gesamtumsatz betrug US$ 3,1 Milliarden. Dabei wuchs der Umsatz mit dem Verkauf von Downloads zweistellig um 19 Prozent, nämlich von US$ 1,7 Milliarden auf US$ 2 Milliarden.

Insgesamt gesehen fielen die Umsätze der US-amerikanischen Musikindustrie jedoch um 12 Prozent auf US$ 7,7 Milliarden. Denn das Wachstum im digitalen Bereich konnte den Rückgang beim Verkauf physischer Datenträger, genauer gesagt dem Verkauf von CDs, der sich 2009 auf 21 Prozent belief, noch immer nicht wettmachen. Auch verzeichnete der Vertrieb von Tonaufnahmen über mobile Endgeräte im Jahr 2009 einen Einbruch um 25 Prozent auf US$ 729 Millionen. Hier ging insbesondere im Bereich des Vertriebs von Klingeltönen, der insgesamt 60 Prozent des mobilen Marktsegments ausmacht, die Nachfrage um 34 Prozent zurück. Demgegenüber schrumpfte der Verkauf mobiler Downloads von Tonaufnahmen nur um fünf Prozent. Ingesamt gesehen stieg jedoch die Nachfrage nach Tonaufnahmen und Musikvideos über mobile Endgeräte etwas an.

2. Deutschland

In Deutschland befindet sich der Musikmarkt nach Angaben des Branchenverbandes, dem Bundesverbandes der Musikindustrie, auf einem „Konsolidierungskurs", vor allem wegen des kontinuierlichen Wachstums im Downloadmarkt und in sogenannten „neuen Geschäftsfeldern", worunter neue Marktsegmente wie u.a. Live-Vorführungen, Merchandising, Künstlermanagement, Brandpartnership, werbefinanzierten Streamingdienste und Abonnementmodelle verstanden werden.[483] Letztere finden in der offiziellen Statistik des Bundesverbandes der Musikindustrie erstmals für die Jahre 2008 und 2009 Erwähnung.

Insgesamt gesehen verbuchte der deutsche Musikmarkt auch im Jahr 2009 einen Rückgang von 2,1 Prozent, d.h. schrumpfte das Gesamtvolumen von EUR 1,84

482 Quelle aller nachfolgend erwähnter Zahlen: RIAA, 2009 Year-End Shipment Statistics, http://76.74.24.142/A200B8A7-6BBF-EF15-3038-582014919F78.pdf (zuletzt abgerufen am 01.07.2010).

483 *Bundesverband der Musikindustrie*, Musikindustrie in Zahlen 2009, S. 12.

Milliarden im Jahr 2008 auf EUR 1,80 Milliarden im Jahr 2009.[484] Der Verkauf von Tonträgern einschließlich Downloads ging um 3,3 Prozent zurück. Die hieraus resultierenden Verluste konnten teilweise durch den Anstieg der Einnahmen aus den neuen Geschäftsfeldern um 11 Prozent – von EUR 110 Millionen auf EUR 122 Millionen – ausgeglichen werden. Dieser Bereich machte damit am Gesamtumsatz einen Anteil von sechs Prozent aus, wobei der Löwenanteil durch Einnahmen aus Live-Aufführungen, Merchandising und Künstlermanagement generiert wurde. Der Verkauf physischer Datenträger stellt mit 78 Prozent weiterhin den mit Abstand größten Teil am Gesamtumsatz dar. [485] Downloads von Tonaufnahmen über das Internet und über mobile Endgeräte repräsentieren mit sieben Prozent mittlerweile den zweitgrößten Posten der in der Musikindustrie erzielten Einnahmen.[486]

Der Markt für Downloads entwickelt sich in Deutschland zwar langsamer als erwartet, wächst aber stetig. So betrug der Anteil von Downloads an den Musikverkäufen über sämtliche Medien im Jahr 2009 acht Prozent und damit zwei Prozent mehr als im Vorjahr.[487] Der mit Downloads erzielte Umsatz stieg im Vergleich zum Vorjahr um 34,6 Prozent von EUR 87,9 Millionen auf 118,2 Millionen. Auch entfielen im Jahr 2009 erstmals ein größerer Teil der Umsätze auf Downloads von *bundles*[488] als auf Downloads einzelner Musiktitel. Abgesehen von dem Verkauf von Downloads nimmt das Internet als Vertriebskanal generell eine immer wichtigere Position ein. So wurden mit Musikdownloads, dem internetgestützten Versand von CDs und mobilen internetbasierten Angeboten im Jahr 2009 erstmals höhere Umsätze erzielt als mit allen anderen Handelsformen, insbesondere dem Vertrieb über Elektrofachmärkte.[489] Fast jeder dritte Euro, der in der Musikbranche verdient wird, steht damit im Zusammenhang mit dem Internet.

Aufgrund der positiven Entwicklung im Downloadmarkt und in den neuen Geschäftsfeldern geht der Branchenverband davon aus, dass der heiß ersehnte Wendepunkt in der Musikindustrie hin zu einem Wachstum nicht – wie bisher erwartet[490] – erst im Jahr 2013, sondern bereits im Jahr 2011 erreicht werden könnte.[491] Dabei wird davon ausgegangen, dass die notwendigen Wachstumsimpulse

484 *Bundesverband der Musikindustrie* s.o.
485 *Bundesverband der Musikindustrie*, Musikindustrie in Zahlen 2009, S. 13.
486 Die restlichen acht Prozent werden durch Einnahmen im Zusammenhang mit Leistungsschutzrechten generiert.
487 *Bundesverband der Musikindustrie*, Musikindustrie in Zahlen 2009, S. 13/14.
488 Vgl. 4. Kapitel, Teil B.III.2.
489 *Bundesverband der Musikindustrie*, Musikindustrie in Zahlen 2009, S. 34.
490 Nach einer im September 2009 vorgestellten Studie der Gesellschaft für Konsumforschung („GfK") ging der Bundesverband bisher davon aus, dass die digitalen Märkte die Ausfälle aus dem Verkauf physischer Datenträger erst ab dem Jahr 2013 kompensieren und ab diesem Zeitpunkt für den Gesamtmarkt Wachstumsimpulse setzen würden. Bis zu diesem Zeitpunkt wurde erwartet, dass der physische Markt weiterhin jährlich um etwa 5 Prozent

vor allem aus dem Verkauf digitaler Alben sowie aus Abonnementmodellen, zugangsgebundenen Musikangeboten und verstärkten Einnahmen aus den Lizenzgeschäften für Streamingangebote (d.h. Kooperationen mit Internetdiensten wie MySpace und YouTube) kommen werden. [492]

D. DRM-Systeme im Filmbereich

Auch die Filmindustrie steht den Auswirkungen der Digitalisierung mit Skepsis gegenüber.[493] Fraglich ist, ob dies zu ähnlichen Folgen führen wird, wie sie die anfängliche Ablehnung der Digitalisierung durch die Musikindustrie für diesen Industriezweig nach sich gezogen hat.

I. Marginal entwickelter Online-Vertrieb

Der Markt für den Online-Vertrieb von Filmwerken ist bisher – ebenso wie dies lange Zeit im Musikbereich der Fall war – noch wenig entwickelt, d.h. es gibt nur wenige Dienste, die den Nutzern den direkten Download von Filmwerken über das Internet erlauben. Daher macht der digitale Vertrieb von Filmen über das Internet in den USA gerade einmal fünf Prozent des Gesamtumsatzes der Branche aus.[494] Denn bisher weigern sich vor allem die großen Hollywood-Studios, ihre Filme einfach, schnell und ohne den Einsatz von DRM-Systemen über das Internet zum Kauf oder zur vorübergehenden Nutzung (vergleichbar dem Videoverleih) zur Verfügung zu stellen. Die Angebote der wenigen existierenden Anbieter sind im Vergleich zu der Menge an Filmen, die auf DVD erworben werden können, extrem beschränkt; so bietet der iTunes-Store ca. 1.000, der Einzelhändler Amazon weniger als 5.000 und der auf Filme spezialisierte Dienst Netflix etwa 6.000 Filme an.[495] Weiterhin können die Filme nur über bestimmte, das DRM-System des jeweiligen Anbieters unterstützende digitale Endgeräte abgespielt werden, da auch

schrumpfen, hingegen die digitalen Märkte um 17 Prozent wachsen würden, vgl. *Bundesverband der Musikindustrie*, GFK Musikmarktprognose 2009, 17.09.2009, abrufbar unter http://www.musikindustrie.de/fileadmin/news/presse/090917_Musikmarktprognose_FINAL_dk.pdf (zuletzt abgerufen am 01.07.2010).

491 *Bundesverband der Musikindustrie*, Musikindustrie in Zahlen 2009, S. 16.

492 *Bundesverband der Musikindustrie* s.o.

493 Vgl. 3. Kapitel, Teil A.II.

494 *IFPI*, IFPI Digital Music Report 2010 – Key Highlights, S. 1, http://www.ifpi.org/content/library/DMR2010_KEY_HIGHLIGHTS.pdf (zuletzt abgerufen am 01.07.2010.).

495 *Rose*, Dear Hollywood Studios: Let My Video Go, WIRED, 25.02.2008, www.wired.com/entertainment/hollywood/magazine/16-03/st_essay (zuletzt abgerufen am 01.07.2010).

beim Vertrieb über das Internet die CSS-DRM-Technologie eingesetzt wird.[496] Dieses DRM-System ist sehr restriktiv und räumt den Nutzern keinerlei Spielraum bei der Nutzung digitaler Filme ein, weder in Bezug auf die Herstellung von Sicherungskopien noch in Bezug auf die Bearbeitung zu nicht-kommerziellen Zwecken.[497]

II. Unterschiedlich geprägte Nutzererfahrungen im Hinblick auf DRM-Systeme

Hinsichtlich des Einsatzes von DRM-Systemen im Zusammenhang mit dem digitalen Vertrieb von Filmwerken besteht jedoch ein wesentlicher Unterschied zur Musikindustrie, da die Nutzer von Seiten der Filmindustrie in der Vergangenheit an einen anderen Umfang der Nutzbarkeit von Filmen gewöhnt wurden als in Bezug auf Tonaufnahmen. Im Gegensatz zu Tonaufnahmen, die die Nutzer in Form von CDs dauerhaft zu Eigentum erwerben und hierüber aufgrund des Fehlens von Einschränkungen durch DRM-Systeme relativ frei verfügen können, sind die Nutzer bei Filmwerken seit Jahren daran gewöhnt, einerseits Filme über einen Filmverleih nur auszuleihen, d.h. nach Ablauf einer bestimmten Zeit die jeweilige Kopie des Films wieder zurückzugeben, und andererseits über Filme, die sie in Form einer Videokassette oder einer DVD dauerhaft zu Eigentum erwerben, aufgrund der insoweit eingesetzten CSS-DRM-Technologie nur eingeschränkt verfügen zu können, d.h. insbesondere keine Kopien herstellen zu können.[498]

Da die Erwartungshaltung der Nutzer in dieser Weise vorgeprägt sind, ist davon auszugehen, dass die Nutzer im Filmbereich eine höhere Toleranz in Bezug auf DRM-gestützte Einschränkungen der Nutzbarkeit von digitalen Filmwerken zeigen würden.[499]

496 *Bangeman*, DRM (on music) is dead. Long live DRM (on video)!, Ars Technica, 08.01.2008, http://arstechnica.com/news.ars/post/20080108-drm-is-dead-for-music.html (zuletzt abgerufen am 01.07.2010).

497 *CDT*, Evaluating DRM, 2006, S. 5.

498 *Sandoval*, End of the world as Hollywood knows it, CNET News, 20.10.2009, http://news.cnet.com/8301-31001_3-10378654-261.html (zuletzt abgerufen am 01.07.2010).

499 So *Eric Garland*, CEO des auf die Sammlung von Daten in Bezug auf Filesharing-Aktivitäten im Internet spezialisierten Marktforschungsunternehmens Big Champane im Interview mit CNET News, vgl. *Sandoval*, End of the world as Hollywood knows it, CNET News, 20.10.2009, http://news.cnet.com/8301-31001_3-10378654-261.html (zuletzt abgerufen am 01.07.2010). Zum Einfluss der Erwartungshaltung der Nutzer auf die Akzeptanz digitaler Angebote vgl. 5. Kapitel, Teil B.IV.

III. Genereller Anstieg der Download-Aktivitäten im Zusammenhang mit Filmwerken im Internet

Die Filmindustrie zögert jedoch bisher, den Vertrieb von Filmwerken über das Internet aktiv voranzutreiben. Grund hierfür ist das Bestreben, die aufgrund der damit einhergehenden hohen Gewinnmargen sehr lukrativen Einkünfte aus dem Verkauf von DVDs nach Möglichkeit vor einer Beeinträchtigung durch den Download- und Streaming-Markt des Internets zu schützen.[500] Mit dieser Haltung läuft die Filmindustrie jedoch Gefahr, ähnlich negative Folgen heraufzubeschwören, wie sie die Musikindustrie bereits ereilt haben, nämlich die massenweise Abwanderung von Nutzern in illegale Angebote.

Hierfür spricht, dass seit etwa 2008 ein massiver Anstieg illegaler Aktivitäten im Internet in Bezug auf digitale Film- und Fernsehfilme zu beobachten ist.[501] Gerade in den europäischen Ländern, wo auf die Aufführung der US-amerikanischen „Blockbuster" in Filmtheatern und deren Veröffentlichung auf DVD bzw. Blu-Ray-Disc nach wie vor länger gewartet werden muss als in den USA, scheinen auch ganz „normale" Nutzer mehr und mehr dazu überzugehen, nach Filmen in illegalen Quellen im Internet zu suchen, um auf diese Weise ihre künstlich verlängerte Wartezeit zu verkürzen.[502] Generell wird derzeit der höchste Anstieg der sogenannten „new adopter activity", d.h. Aktivitäten im Zusammenhang mit dem Herunterladen und Abrufen von Inhalten über das Internet, im Videobereich verzeichnet, was nach Einschätzung von Experten dazu führen wird, dass die Filmindustrie in den kommenden beiden Jahren bezogen auf die traditionellen Vertriebswege einen fühlbaren Verlust von Publikumsanteilen verzeichnen wird.[503] Allerdings gehen mit der Digitalisierung auch große Chancen für die Filmindustrie einher. Denn das Internet stellt auch für die Filmbranche ein äußerst wertvolles Marketinginstrument dar, das es nach Möglichkeit zu nutzen gilt.[504]

500 *Rose*, Dear Hollywood Studios: Let My Video Go, WIRED, 25.02.2008, www.wired.com/entertainment/hollywood/magazine/16-03/st_essay (zuletzt abgerufen am 01.07.2010).

501 *IFPI*, Digital Music Report 2010, S. 21.

502 *Garland* (s.o. Fn. 500), zitiert bei *Sandoval*, End of the world as Hollywood knows it, CNET News, 20.10.2009, http://news.cnet.com/8301-31001_3-10378654-261.html (zuletzt abgerufen am 01.07.2010).

503 *Garland* (s.o. Fn. 500), zitiert bei *Sandoval*, End of the world as Hollywood knows it, CNET News, 20.10.2009, http://news.cnet.com/8301-31001_3-10378654-261.html (zuletzt abgerufen am 01.07.2010): *„That means that this year or next year is going to be Hollywood's year to really start to lose audience – not just at the fringes but in the regular middle-American living rooms."*

504 *MPAA*, Theatrical Market Statistics 2007, S. 8: *„Internet Plays a Significant Role in Driving People to Movies: The Internet is an important source for movie information. A forthcoming study conducted by the MPAA and Yahoo! found that 73% of U.S. moviegoers use the Internet to conduct research before going to the theater. Also, moviegoers who research online are more likely to see a movie on opening weekend, go to the theater more often, and see some movies more than once in the theater.* "; vgl. hierzu auch 7. Kapitel, Teil A.III.2.c.

IV. Zusammenfassung

Anstatt die Gegebenheiten des digitalen Zeitalters zu akzeptieren und die Nutzer durch attraktive Angebote für den dauerhaften oder zeitlich begrenzten Erwerb von Filmen über das Internet an sich zu binden, scheint sich auch die Filmindustrie beim Vertrieb von Filmen in digitaler Form einseitig an DRM-Systeme und eine restriktive Handhabung von Internetangeboten zum Konsum von Filmen festzuklammern.[505] Denn bisher will auch die Filmindustrie nicht akzeptieren, dass die neuen Gegebenheiten betreffend den Vertrieb, die Vermarktung und den Konsum von Multimediawerken aufgrund der Digitalisierung und Verbreitung des Internets die zu erzielenden Umsätze und Gewinne der Branche in Zukunft möglicherweise geringer ausfallen lassen werden, als dies zu Zeiten der fast vollständigen Kontrolle des Vertriebs von Multimediawerken über physische Datenträger der Fall war.[506] Aufgrund dieser Umstände besteht jedoch die Gefahr, dass sich im Filmbereich über kurz oder lang dasselbe Szenario abspielen könnte wie im Musikbereich, d.h. die massenhafte Abwanderung der Nutzer in illegale Angebote mangels attraktiver legaler Alternativen zum Erwerb von Filmen in digitaler Form über das Internet. Um die Internetpiraterie einzudämmen und für sich eine existenzbedrohende Situation wie diejenige, in der sich die Musikindustrie derzeit befindet, zu verhindern, müssten die Studios daher so viel Material wie möglich so schnell und einfach wie möglich zu fairen Preisen den Nutzern über das Internet zur Verfügung stellen. Hierfür gilt es auch den erheblichen Aufwand der Einholung der Rechte aller Betroffenen (wie beispielsweise Drehbuchautoren, Regisseure, Komponisten, Schauspieler etc.) sowie gegebenenfalls auch rechtliche Auseinandersetzungen mit den Sendern, denen bereits auf Jahre hinaus exklusive Rechte an Filmen eingeräumt

505 *informitiv.com*, Sony Pictures proposes Open Market for Movie protection, 27.08.2008, http://informitv.com/news/2008/08/27/sonypicturesproposes/ (zuletzt abgerufen am 01.07.2010).

506 *Garland* (s.o. Fn. 500), zitiert bei *Sandoval*, End of the world as Hollywood knows it, CNET News, 20.10.2009, http://news.cnet.com/8301-31001_3-10378654-261.html (zuletzt abgerufen am 01.07.2010): *„The cute answer, which probably is the truest answer, is that growing a sector is a privilege and not a right. There is no right size. ... Why do we get to make movies that cost $300 million to make? Because we have found venues where people will spend more than $300 million on the result. If people spend only $50 million, then the price of a movie must be $49 million or less. ... One outcome might mean that in the Digital Age the return on investment on a major International tent-pole franchise is not a billion dollars. It's a quarter of that or a third. Therefore we have to get our costs in line with the market value. When we talk about this in 3 or 5 or 7 years, one thing we will have to concede is costs have to come down. We don't have the total control over the distribution chain that we exploited so well as industries for so long. Without that you can't take advantage of the consumer in the same way."*

wurden, die einem Vertrieb über das Internet entgegenstehen könnten, in Kauf zu nehmen.[507]

Immerhin hat die Filmindustrie vor kurzer Zeit eine Initiative namens „Open Market" gestartet, die es ermöglichen soll, dass Nutzer, die Kinofilme von einem der an der Initiative teilnehmenden Partnerunternehmen erworben haben, über einen „neutralen", d.h. auf allen digitalen Endgeräten installierbaren Player abspielen können, wodurch die Nutzer nicht länger darauf angewiesen wären, dass das von ihnen bevorzugte digitale Endgerät gerade auch das DRM-System des von ihnen zum Erwerb von Filmen genutzten Vertriebshändlers unterstützt.[508] Allerdings scheiterte im Musikbereich eine ähnliche Initiative der Tonträgerunternehmen im Hinblick auf Musikdownloads im Jahr 2004. Vor diesem Hintergrund gilt die Open-Market-Bemühung als ein letzter Versuch der Filmindustrie, das Scheitern von DRM-Systemen auch beim Vertrieb von Filmen über das Internet abzuwenden oder zumindest noch einige Zeit zu verzögern.[509] Jedoch ist bereits aus dem Umstand, dass sich so wichtige Unternehmen wie Apple oder die Walt Disney Studios an der Initiative nicht beteiligt haben, ersichtlich, dass die Filmindustrie bei ihrem Streben nach Interoperabilität und Standardisierung von DRM-Systemen noch einige Hürden zu nehmen haben wird.

6. Kapitel: Ergebnis

> „[S]ome copyright owners may well desire to eliminate the making of any copies of their works, and they may well object to existing legislation and systems that permit users to make copies under certain circumstances. They may wish to replace the existing system with one giant metering system, whereby every act of reproduction would be subject to their technological control. But it would be unwise for policy-makers (and ultimately perhaps for copyright owners) to act as if they were in a vacuum. The fact is that the law authorizes some reproduction and the public has come to have certain expectations regarding its ability to copy. Both legislators and copyright owners risk public

507 So auch *Rose*, Dear Hollywood Studios: Let My Video Go, WIRED, 25.02.2008, www.wired.com/entertainment/hollywood/magazine/16-03/st_essay (zuletzt abgerufen am 01.07.2010).

508 *informitiv.com*, Sony Pictures proposes Open Market for Movie protection, 27.08.2008, http://informitv.com/news/2008/08/27/sonypicturesproposes/ (zuletzt abgerufen am 01.07.2010).

509 *Arrington*, Movie Labels To Launch New „Open Market" Play Anywhere Scheme As Last Ditch Effort To Save DRM, TechCrunch, 26.08.2009, http://www.techcrunch.com/2008/08/26/movie-labels-to-launch-new-open-market-play-anywhere-scheme-as-last-ditch-effort-to-save-drm/ (zuletzt abgerufen am 30.10.2010).

rejection of their efforts to adapt law and practice to the digital world if they ignore these public expectations."[510]

Als Ergebnis bleibt somit festzuhalten, dass DRM-gestützte Modelle zum Vertrieb von Musikdownloads über das Internet gescheitert sind und dieses Scheitern vor allem darin begründet liegt, dass die Interessen der Rechtsinhaber, in diesem Fall hauptsächlich diejenigen der Tonträgerunternehmen, und diejenigen der Nutzer im Rahmen der eingesetzten DRM-Systeme nicht zu einem für die Nutzer akzeptablen Ausgleich gebracht wurden. In dem Glauben, durch gesetzlich vor Umgehung geschützte DRM-Systeme einseitig ihre Interessen auch über die urheberrechtlichen Grenzen hinaus schützen zu können, versäumten es die Rechtsinhaber, den urheberrechtlich legitimierten Interessen der Nutzer bei der Strukturierung der eingesetzten technischen Schutzmaßnahmen ausreichend Rechnung zu tragen. Damit führten die Rechtsinhaber jedoch selbst eine Situation herbei, in der sich die mit der Digitalisierung einhergehenden Nachteile zu ihren Lasten verdoppelten: nicht nur erlitten sie unverändert wirtschaftliche Einbußen aufgrund der unautorisierten Verbreitung ihrer Werke im Internet über illegale Filesharing-Netzwerke, auf die der Einsatz von DRM-Systemen keinen Einfluss zeigte, sondern darüber hinaus konnten sie diese Einbußen auch nicht durch die Etablierung erfolgreicher neuer, internetbasierter Vertriebswege wettmachen. Denn aufgrund des Einsatzes restriktiver, nicht interoperabler DRM-Systeme führte die Nutzung vieler legaler Angebote zu einer Frustration der Nutzer, die folglich keine ausreichenden Anreize für sich sahen, solchen legalen Angebote den Vorzug vor illegalen Filesharing-Netzwerken zu geben. Dieses Dilemma fasste Tim Wu, Professor an der Columbia Law School, wie folgt zusammen: „digitale Schlösser sind kein Ersatz für ein gutes Geschäftsmodell."[511] Langsam scheint die Musikindustrie dieses Dilemma jedoch zu erkennen, weswegen sie sich beim Vertrieb von Musikdownloads zum Verzicht auf den Einsatz „digitaler Schlösser" entschlossen hat und sich seit etwa zwei Jahren mehr und mehr aktiv darum bemüht, neue, für die Nutzer attraktive Geschäftsmodelle zum Vertrieb von Musikprodukten zu finden, die die Interessen der Nutzer mehr als bisher berücksichtigen und daher eine größere Aussicht bieten, in Zukunft den Rückgang beim Verkauf von Tonaufnahmen in Form von physischen Datenträgern zu kompensieren.

Für das Urheberrecht bedeutet diese Entwicklung, dass sich die Vorhersagen, wonach der Einsatz von DRM-Systemen im digitalen Bereich zu einer weitgehen-

510 *Vinje*, EIPR 1996, 431, 432.

511 Diese und die folgenden Stellungnahmen *Wu*'s stammen aus einer im Technologie-Weblog der New York Times geführten Diskussion zwischen *Wu* und dem General Counsel von NBC Universal, *Rick Cotton*, vgl. *Hansell*, Bits Debate: Is Copyright Protection Needed or Futile?, New York Times Weblog, 14.01.2008, http://bits.blogs.nytimes.com/2008/01/14/bits-debate-is-copy-protection-needed-or-futile/ (zuletzt abgerufen am 01.07.2010); so auch *Lehmann*, in: FS. Pagenberg, 2006, 413, 415; *Hilty*, MMR 2002, 577, 578.

den Verdrängung und Ersetzung des Urheberrechts führen und an dessen Stelle ein einseitig durch die Rechtsinhaber geschaffenes *self executing law* treten würde, nicht bewahrheitet haben. Denn aufgrund der wesentlichen Eigenschaft des Zeitalters der Digitalisierung, nämlich der jedem Nutzer mit Hilfe durchschnittlicher technischer Hilfsmittel wie Computer und Internet offenstehenden Möglichkeit der Herstellung und weltweiten Verbreitung einer unbegrenzten Anzahl von digitalen Kopien von Multimediawerken, kombiniert mit dem Phänomen des *analog hole*, war das Vorhaben der Rechtsinhaber, durch technische Schutzmaßnahmen die effektive Kontrolle über die Verbreitung digitaler Multimediawerke wiederherzustellen, von vornherein zum Scheitern verurteilt. Praktisch bedeutet dies, dass jedes Geschäftsmodell zum Vertrieb von digitalen Multimediawerken im Zeitalter der Digitalisierung zu jeder Zeit in Konkurrenz mit der Möglichkeit einer unautorisierten Verbreitung dieser Werke über das Internet steht, da sich diese Möglichkeit auch durch den Einsatz technischer Schutzmaßnahmen nicht beseitigen lässt. Es gilt somit, diese faktische Konkurrenz nach den Regeln des wirtschaftlichen Wettbewerbs, d.h. durch eine höhere Attraktivität legaler Angebote zu schlagen. Die Lösung des digitalen Dilemmas liegt somit nicht in der Perfektionierung des technischen Schutzes gegen die unautorisierte Verbreitung digitaler Multimediawerke, sondern in der Schaffung von mit der illegalen Konkurrenz konkurrenzfähigen Angeboten.[512]

Bei der Schaffung dieser wettbewerbsfähigen Angebote können und müssen DRM-Systeme, die die Abwicklung von Transaktionen über das Internet wie beispielsweise die Einrichtung und Bezahlung eines Musikabonnements technisch ermöglichen, auch in Zukunft eine Rolle spielen. Allerdings muss der Einsatz solcher DRM-Systeme zukünftig seine Grenze dort finden, wo die legitimen Interessen der Nutzer beeinträchtigt und diese folglich in die Nutzung illegaler Angebote zurückgetrieben werden würden. In diesem Zusammenhang spielt die Erwartungshaltung der Nutzer eine wesentliche Rolle, die vor allem durch die Erfahrungen der Nutzer im Umgang mit Multimediawerken aus der Vergangenheit und damit auch durch das Bewusstsein geprägt ist, welche Befugnisse das Urheberrecht ihnen in Bezug auf den Umgang mit urheberrechtlich geschützten Werken grundsätzlich einräumt. Daraus folgt jedoch, dass die Regelungen des Urheberrechts, insbesondere die urheberrechtlichen Schrankenbestimmungen zugunsten der Nutzer, auch im digitalen Zeitalter weiterhin eine wichtige Rolle spielen werden. Zudem ist das Urheberrecht ein wesentlicher Faktor für die Ahndung von Urheberrechtsverlet-

512 So im Ergebnis auch *Mittenzwei,* Informationen zur Rechtewahrnehmung, 2006, S. 23; m.E. *Ünlü*, Content Protection, 2005, S. 4, 9; *Perritt*, Music Markets and Mythologies, S. 11; *Schmidt*, Ohne Kopierschutz mehr Umsatz, Frankfurter Allgemeine Zeitung, 03.03.3008, S. 15, abrufbar unter http://www.faz.net/s/RubE2C6E0BCC2F04DD787CDC274993E94C1/Doc~EDCAB4B2561C64E25AAF65B87BB8BF5B8~ATpl~Ecommon~Scontent.html (zuletzt abgerufen am 01.07.2010).

zungen. Denn aus der Tatsache, dass urheberrechtswidriges Verhalten im Zeitalter der Digitalisierung absehbar auch durch den Einsatz von DRM-Systemen nicht vollumfänglich beseitigt werden kann, ergibt sich, dass das urheberrechtliche Instrumentarium zur Durchsetzung urheberrechtlicher Rechtspositionen bis auf weiteres alternativlos bleiben wird.

Teil 3:
Bekämpfung von Urheberrechtsverletzungen im Web 2.0 durch Content-Identification-Technologien

Mit der Ankunft des Web 2.0 haben sich die Herausforderungen für den Schutz und die Kommerzialisierung urheberrechtlich geschützter Werke noch einmal erhöht. Denn durch die in diesem Zuge entstandenen neuen Internetdienste und -plattformen (nachfolgend „Web 2.0-Dienste") werden den Nutzern vielfältige neue Wege eröffnet, digitale Inhalte über das Internet der Öffentlichkeit zugänglich zu machen. Ihrem Ursprung nach beabsichtigten Web 2.0-Dienste zwar vor allem, es den Nutzern zu ermöglichen, die Früchte ihrer *eigenen* Kreativität über das Internet zu veröffentlichen und zu verbreiten; mit der zunehmenden Popularität dieser Dienste wurden diese jedoch von den Nutzern mehr und mehr dazu benutzt, um fremde Inhalte, insbesondere professionell erstellte, populäre digitale Multimediawerke, im Original oder in bearbeiteter Form ohne Erlaubnis der Rechtsinhaber der Öffentlichkeit zugänglich zu machen.

Um dieser Missbrauchsanfälligkeit von Web 2.0-Diensten zu begegnen, werden innerhalb dieser Dienste immer häufiger Technologien eingesetzt, die feststellen können, ob es sich bei einem von einem Nutzer hochgeladenen digitalen Inhalt um ein urheberrechtlich geschütztes Multimediawerk handelt. Diese Technologien werden zusammenfassend als Content-Identification-Technologien bezeichnet, worunter in der Regel sowohl Wasserzeichentechnologien[513] als auch sogenannte „digital fingerprinting technologies" verstanden werden. Die vorliegende Arbeit konzentriert sich auf letztere Art von Technologien, deren technische Grundlagen, Funktionen und mögliche Einsatzgebiete nachfolgend dargestellt werden, weswegen unter dem Begriff der Content-Identification-Technologien im Rahmen dieser Arbeit ausschließlich *digital fingerprinting technologies* zu verstehen sind.

Der Einsatz von Content-Identification-Technologien wird von Seiten der Rechtsinhaber immer stärker propagiert und stellt, spätestens seit der Klage des Medienkonzerns Viacom gegen die Videoplattform YouTube, für die Anbieter von Internetdiensten zunehmend eine ökonomischen Notwendigkeit dar, eine „cost of doing business".[514] Dementsprechend entwickelte sich über die letzten Jahren ein eigener Markt für solche technologischen Instrumente, die teils miteinander kon-

513 Vgl. 4. Kapitel, Teil B.II.2.

514 *Germain*, Dusting for Copyright Clues With Digital Fingerprinting Tech, TechNewsWorld, 22.08.2008, http://www.technewsworld.com/rsstory/64249.html (zuletzt abgerufen am 01.07.2010).

kurrierend, teils einander ergänzend dazu eingesetzt werden, um digitale Multimediawerke im Internet zu identifizieren und im Anschluss daran entweder aus Internetdiensten zu entfernen oder aber die Nutzung eines solchen Werks im Rahmen dieses Dienstes zu überwachen und vor allem durch die Zuschaltung von Werbung zu kommerzialisieren.[515]

Aus rechtlicher Perspektive stellt sich im Zusammenhang mit dem Einsatz dieser Technologien und den damit einhergehenden Möglichkeiten, den in Web 2.0-Diensten stattfindenden Datenverkehr zu kontrollieren, vor allem die Frage, welche Konsequenzen sich hieraus für die Anwendbarkeit der eigens für die Anbieter von Internetdiensten geschaffenen Haftungsbeschränkungen ergeben. Denn die Haftungsbeschränkungen des US-amerikanischen, europäischen und deutschen Rechts basieren unter anderem auf der Annahme, dass den Anbietern von Internetdiensten eine effektive inhaltliche Kontrolle des innerhalb ihrer Dienste abgewickelten Datenverkehrs technisch unmöglich ist. Vor allem die Rechtsinhaber stellen sich jedoch zunehmend auf den Standpunkt, dass ISPs mehr gegen Urheberrechtsverletzungen unternehmen müssen, da sie hierzu aufgrund der neuen Möglichkeiten, die Content-Identification-Technologien insoweit eröffnen, hierzu am besten in der Lage sind. Zu prüfen, ob diese Forderung nach der derzeitigen US-amerikanischen und deutsch-europäischen Rechtslage auch eine rechtliche Grundlage hat, ist Gegenstand des dritten Teils dieser Arbeit.

7. Kapitel: Der Einsatz von Content-Identification-Technologien im Web 2.0

> „We are at a moment of important ambiguity in the balance between copyright enforcement and civil liberties. For the past several years, we have seen a barrage of headlines predicting the fall of the music industry due to digital piracy. Today, as we watch the industry shift to accommodate new models for content distribution, we also see the growth of less prominent and invasive forms of surveillance, filtering and monitoring to guard against potential piracy.“[516]

515 So *Scott Teissler*, Chief Technology Officer für Turner Broadcasting System, zitiert bei *Steinert-Threlkeld*, YouTube's video ID system: is 75 percent good enough?, in: ZDNet Undercover: YouTube's Video Identification System, November 2008, S. 13. Nach einer Studie des Markforschungsinstituts MultiMedia Intelligence vom Januar 2008 ist für den Markt für Content-Identification-Technologien auch in Zukunft ein stetiges Wachstum zu erwarten, so dass dieser bis zum Jahr 2012 weltweit ein Volumen von mehr als einer halben Mrd. Dollar erreichen wird, vgl. *Rosenblatt*, New Market Study Predicts Growth in Watermarking and Fingerprinting Markets, 24.01.2008, http://www.drmwatch.com/watermarking/article.php/3723626 (zuletzt abgerufen am 01.07.2010).

516 *Katyal*, 32 Colum. J.L. & Arts, 401, 425 (2009).

In diesem Kapitel wird zunächst das Phänomen des Web 2.0 beschrieben sowie die darin eine tragende Rolle spielenden Internetdienste vorgestellt. Desweiteren werden die technischen Grundlagen und potentiellen Anwendungsbereiche von Content-Identification-Technologien herausgearbeitet sowie die Kommerzialisierungsmöglichkeiten, die das Web 2.0 bietet, illustriert.

A. Fortentwicklung des Internets zum sogenannten Web 2.0

I. Definition „Web 2.0" und „User Generated Content"

Der Begriff „Web 2.0" bezeichnet die neue, partizipative Dimension des Internets, in der ein durchschnittlicher Nutzer in der Lage ist, Inhalte ohne Mitwirkung althergebrachter Intermediäre wie beispielsweise TV-Sender, Filmstudios oder Tonträgerunternehmen der Öffentlichkeit zugänglich zu machen und an andere interessierte Nutzer weltweit zu verbreiten.[517] Die im Web 2.0 tätigen Intermediäre erfüllen somit nicht die Aufgabe, selbst Inhalte im Internet zur Nutzung bereit zu stellen, sondern geben vielmehr den Nutzern (nur) die erforderlichen Werkzeuge an die Hand, damit diese selbst Inhalte über das Internet anderen Nutzern (öffentlich) zugänglich machen können.[518] Im Web 2.0 sind die Nutzer somit nicht mehr nur passive Nutzer und Zuschauer der im Internet präsentierten Informationen und Inhalte, sondern erschaffen diese selbst und präsentieren sie anderen Nutzern, die auf dieser Grundlage wiederum etwas Neues kreieren können.[519] Dieser „user generated content",[520] der die unterschiedlichsten medialen Ausdrucksformen beispielsweise eines Schrift-, Musik- oder Filmwerks annehmen bzw. aus einer Kom-

517 *Meyers*, 26 Cardozo Arts & Entertainment L. J. 935 (2009).

518 *Ginsburg*, 50 Ariz. L. Rev. 577, 578 (2008); *OECD*, Web 2.0, 2007, S. 9; *Lee*, 2008 U. Ill. L. Rev. 1459, 1500 (2008).

519 *Lee*, 2008 U. Ill. L. Rev. 1459, 1501 (2008).

520 Eine frühe Ausprägung dessen, was gegenwärtig als nutzergenerierte Inhalte bezeichnet wird, ist die sog. „fan fiction", d.h. von Fans geschriebene Fortsetzungen eines populären urheberrechtlich geschützten literarischen Werks, die im Internet unter der Mitarbeit einer Vielzahl von Fans erschaffen und verbreitet werden, oftmals mit Unterstützung des Urhebers des Ursprungswerks, für den dieses Phänomen ein willkommenes Instrument zur weiteren Vermarktung seines Werks darstellt. Eine 2008 von der Unternehmensberatung Deloitte Touche Tohmatsu durchgeführten Umfrage ergab, dass von 2.000 befragten Nutzern im Alter zwischen 13 und 75 bereits die Hälfte im Internet schon einmal eigene Inhalte in Form von Fotos oder Videos zugänglich gemacht bzw. eine Webseite mit eigenen Inhalten erstellt hat, was bedeutet, dass UGC mittlerweile Teil der alltäglichen Nutzung des Internets und damit zu einem Massenphänomen geworden ist. Auch steht zu erwarten, dass die Verbreitung von UGC noch weiter zunehmen wird, da es immer mehr Unternehmen gibt, die Anwendungsprogramme für das Web 2.0 entwickeln und den Nutzern im Internet zur Verfügung stellen. Vgl. *Montagnani*, 26 Cardozo Arts & Ent. L.J. 719, 769 (2009); *Lee*, 2008 U. Ill. L. Rev. 1459, 1461, 1500 (2008).

bination derselben bestehen kann,[521] wird in Weblogs, durch Podcasts, auf Videoplattformen oder in sozialen Netzwerken wie Facebook oder MySpace eingestellt, veröffentlicht und verbreitet.[522]

Weiterhin können sich die Nutzer des Web 2.0 als Kommentatoren und Kritiker von digitalen Inhalten betätigen, sowie die bereitgestellten Internetdienste und –software ihren Vorstellungen entsprechend anpassen und fortentwickeln.[523] Neben der Möglichkeit, in bisher unbekanntem Umfang als Privatperson selbst gestaltend im Internet tätig zu werden, besteht die Attraktivität des Web 2.0 vor allem darin, über nutzergenerierte Inhalte soziale Netzwerke aufzubauen oder daran teilzuhaben.[524] Dies zeigt sich insbesondere daran, dass die meisten Internetdienste, die es im Web 2.0 innerhalb kurzer Zeit zu erheblicher Popularität gebracht haben, wie beispielsweise YouTube, Facebook und MySpace, mit sogenannten „social networking"-Funktionen arbeiten, die es den Nutzern ermöglichen, mit anderen Nutzern in Kontakt zu treten und mit ihnen Informationen und Inhalte auszutauschen.[525]

In den Anfängen des Web 2.0 wurden mit nutzergenerierten Inhalten und Web 2.0-Diensten in der Regel keine kommerziellen Zwecke verfolgt.[526] Spätestens seit der US$ 1,65 Milliarden teuren Akquisition der Web 2.0-Videoplattform YouTube durch den Suchmaschinengiganten Google bestehen jedoch keine Zweifel mehr daran, dass das Web 2.0 mittlerweile im Zentrum wirtschaftlicher Interessen von Medienunternehmen steht. Zwar sind nutzergenerierte Inhalte auch gegenwärtig in der Regel immer noch kostenlos zugänglich, d.h. die Nutzer zahlen weder dafür, dass sie von anderen Nutzer erstellte bzw. öffentlich zugänglich gemachte Inhalte konsumieren, noch erhalten sie eine Vergütung dafür, wenn sie selbst Inhalte erschaffen und diese innerhalb von Web 2.0-Diensten anderen Nutzern zugänglich machen. Jedoch wird die Trennlinie zwischen Internetdiensten mit nutzergenerierten Inhalten, die keinerlei kommerzielle Absichten verfolgen, und kommerzialisierten Angeboten zunehmend unscharf, vor allem durch die im Web 2.0 zunehmend verbreiteten werbebasierten Internetdienste („ad-supported business models").[527] Diese zunehmende Kommerzialisierung von Web 2.0-Diensten führt beispielsweise dazu, dass ein Nutzer, der ein selbst hergestelltes Multimediawerk innerhalb eines Web 2.0-Dienstes öffentlich zugänglich macht, von einem Unternehmen „entdeckt" werden und in der Folge einen Vertrag betreffend die Produk-

521 *OECD*, Web 2.0, 2007, S. 17.
522 Grünbuch Urheberrechte in der wissensbestimmten Wirtschaft, KOM(2008) 466/3, S. 19.
523 *OECD*, Web 2.0, 2007, S. 17.
524 *Lee*, 2008 U. Ill. L. Rev. 1459, 1501 (2008).
525 *Lee*, s.o.
526 *OECD*, Web 2.0, 2007, S. 10.
527 *Lee*, 2008 U. Ill. L. Rev. 1459, 1503 (2008); *OECD*, Web 2.0, 2007, S. 10; vgl. 7. Kapitel, Teil A.III.2.d.

tion und Vermarktung seines Werkes erhalten kann.[528] Auch stellen Unternehmen der Multimediaindustrie vermehrt ihre Multimediawerke in Web 2.0-Diensten ein, um auf diese Weise vom Phänomen der sogenannten „superdistribution" zu profitieren, d.h. der Verbreitung des Werks von Nutzer zu Nutzer und den damit erzielten Marketingeffekten.

II. Typische Internetdienste des Web 2.0

Typische Ausprägungen von Web 2.0-Diensten sind Videoplattformen und Soziale Netzwerke, die nachfolgend kurz vorgestellt werden.

1. Videoplattformen

a. Allgemein

Durch die Videoplattformen des Web 2.0 wurde der Zugang zu Filmwerken im Internet revolutioniert. Hintergrund dieser Entwicklung war einerseits das explosionsartige Wachstum des Internets durch die zunehmende Verbreitung von Breitbandanschlüssen und andererseits der gesellschaftliche Trend, wonach das Ausleben der eigenen Kreativität und die Erschaffung eigener multimedialer Inhalte in den Vordergrund rückt und sich die Nutzer mehr und mehr vom passiven Konsum vorgefertigter Inhalte emanzipieren.[529] Videoplattformen bringen traditionelle Unternehmen der Multimediaindustrie in zweierlei Hinsicht in Bedrängnis. Zum einen erhöhen sie die Menge an im Internet verfügbaren multimedialen Inhalten, unter denen ein Nutzer auswählen kann, und verschärfen damit den Wettbewerb um die Aufmerksamkeit der Nutzer. Zum anderen beeinflussen sie maßgeblich die Strukturen betreffend den Vertrieb und die Vermarktung von multimedialen Inhalten.[530] Vor allem sieht sich die Filmindustrie jedoch durch das verstärkte Auftreten von Videoplattformen mit der Tatsache konfrontiert, dass auch sie – ebenso wie die Musikindustrie – zunehmend die Kontrolle darüber verliert, wo, wann und in welcher Form Nutzer Filmwerke im Internet konsumieren.[531]

528 *Lee*, s.o.
529 *Meisel*, Journal of Internet Law, Volume 12, Number 8, Februar 2009, 1, 8.
530 *Meisel*, Journal of Internet Law, Volume 12, Number 8, Februar 2009, 1, 9; zu den hierdurch eröffneten neuen Vermarktungsmöglichkeiten vgl. 7. Kapitel, Teil A.III.2.c.
531 *Meisel*, Journal of Internet Law, Volume 12, Number 8, February 2009, 1, 15.

b. YouTube

Die weltweit populärste Videoplattform ist gegenwärtig der Web 2.0-Dienst YouTube. Auf der Webseite www.youtube.com können die Nutzer kurze[532] Film- und Videowerke (nachfolgend „Videoclips"), hochladen, ansehen und andere hierauf aufmerksam machen. Mittlerweile bietet YouTube zudem Funktionen an, über die Nutzer auch HD-Videoclips auf der Plattform einstellen und Videoclips über ihre Fernseher abspielen können.[533] Der Web 2.0-Dienst wurde im Februar 2005 von Chad Hurley, Steve Chen und Jawed Karim mit dem Ziel gegründet, das Hochladen von Videoclips ins Internet ebenso einfach wie einen Telefonanruf zu machen. Das erste Video wurde am 23. April 2005 auf der Webseite eingestellt. Aufgrund seiner Bedienfreundlichkeit avancierte YouTube innerhalb kürzester Zeit zum Massenphänomen und wurde bereits im Oktober 2006 zu dem bis dato für Web 2.0-Dienste kaum vorstellbaren Preis von US$ 1,65 Milliarden von dem Suchmaschinenanbieter Google erworben, nachdem dessen Videoplattform „Google Video" sich am Markt nicht wunschgemäß etabliert hatte.[534]

Auf YouTube werden täglich mehr als eine Milliarde Videoabrufe von den etwa 330 Millionen Nutzern weltweit getätigt, die das Portal monatlich besuchen.[535] Pro Minute werden auf den Web 2.0-Dienst etwa dreizehn Stunden Material hochgeladen.[536] Laut dem Marktforschungsinstitut Alexa gehört YouTube damit zu den am häufigsten besuchten Internetseiten weltweit, lediglich übertroffen durch Google, Yahoo und Facebook.[537] Nach Angaben des Marktforschungsunternehmens ComScore hält YouTube in den USA konstant einen Marktanteil von 40 Prozent, und ist damit unangefochtener Branchenprimus im Bereich Videoplattformen.[538]

532 Auf YouTube ist die Länge eines Videoclips, der auf die Plattform hochgeladen werden kann, auf zehn Minuten begrenzt, u.a. um dadurch das Hochladen vollständiger urheberrechtlich geschützter Filme, TV-Shows und Folgen von TV-Serien zu erschweren, vgl. *Meisel*, Journal of Internet Law, Volume 12, Number 8, February 2009, 1, 15, Fn. 6.

533 *Heise Online*, YouTube: Über 1 Milliarde Videoabrufe pro Tag, 11.10.2009, http://www.heise.de/newsticker/meldung/YouTube-Ueber-1-Milliarde-Videoabrufe-pro-Tag-821259.html (zuletzt abgerufen am 01.07.2010).

534 *Heise Online*, Google kauft Online-Video-Seite YouTube, 10.10.2006, http://www.heise.de/newsticker/meldung/Google-kauft-Online-Video-Seite-YouTube-169658.html (zuletzt abgerufen am 01.07.2010).

535 *Heise Online*, YouTube: Über 1 Milliarde Videoabrufe pro Tag, 11.10.2009, http://www.heise.de/newsticker/meldung/YouTube-Ueber-1-Milliarde-Videoabrufe-pro-Tag-821259.html (zuletzt abgerufen am 01.07.2010); *ohne Autor*, Soziale Netzwerke vor der Gewinnschwelle, Frankfurter Allgemeine Zeitung, 29.9.2009, S. 23.

536 *Steinert-Threlkeld*, ZDNet Undercover: YouTube's Video Identification System, November 2008, S. 2.

537 *Ohne Autor*, Google will mit Youtube endlich Geld einnehmen, Frankfurter Allgemeine Zeitung, 21.8.2009, S. 17.

538 *McCarthy*, ComScore: 100 million YouTube viewers in October, CNET News, 10.12.2008, http://news.cnet.com/8301-1023_3-10120027-93.html?part=rss&tag=feed&subj=News-DigitalMedia (zuletzt abgerufen am 01.07.2010).

Dahinter folgen Fox Interactive mit MySpaceTV, Yahoo, Microsoft, Viacom und schließlich die als Joint Venture von News Corp. und NBC Universal betriebene Plattform Hulu.[539] In Deutschland wird YouTube monatlich von ca. 15 Millionen Nutzern abgerufen[540] und ist damit nach einer Untersuchung des Markforschungsunternehmens ComScore auch hier gegenwärtig das populärste Videoportal.[541] Darauf folgen die Videoseiten der Unternehmen ProSiebenSat.1 (Sevenload), RTL Group (Clipfish) und Fox Interactive Media (MySpace). Weit dahinter liegen die Videoangebote der Axel Springer AG und der Deutschen Telekom.

YouTube verwendet für seine Videoplattform hauptsächlich den Apache HTTP-Webserver, sowie zur Speicherung von Bildern und anderer statischer Inhalte den freien Webserver Lighttpd. Die Videoclips, die in verschiedenen Formaten (beispielsweise AVI, MPEG, WMV, Quicktime) auf die Webseite hochgeladen werden können, werden im Flash-Video-Format abgespeichert und können von den Nutzern, während sie im Internet sind, als Stream in ihrem Webbrowser angesehen werden, vorausgesetzt, das für alle gängigen Webbrowser kostenlos im Internet verfügbare Adobe-Flash Plug-in wurde zuvor auf dem Computer des Nutzers installiert. Als weitere Funktionen bietet YouTube eine Suchfunktion, die es den Nutzern ermöglicht, sämtliche auf der Plattform derzeit vorhandene Dateien durch das Eingeben von Begriffen in einer Suchmaske zu durchsuchen, sowie die Möglichkeit, Dritte durch Versendung eines Links, durch den der Adressaten an den Ort auf der Plattform gelangt, an dem der jeweilige Videoclip abgespeichert ist, auf bestimmte Inhalte aufmerksam zu machen; auch kann ein Videoclip auf der Webseite eines Nutzers eingebaut werden („embedded video“).[542]

Bevor ein Nutzer einen Videoclip auf die Plattform hochladen kann, muss er sich registrieren und YouTubes Nutzungsbedingungen akzeptieren, die unter anderem Bestimmungen über den zulässigen Inhalt von „Nutzerübermittlungen“ enthalten.[543] Demnach dürfen auf der Plattform keine Videodateien eingestellt werden, die die Rechte Dritter verletzen. Rechtswidrige Videodateien, die entgegen

539 Zu beiden Konzernen gehören Filmstudios, im Falle von NBC Universal die Universal Studios und im Falle von News Corp. das Hollywood-Studio 20th Century Fox, weswegen Hulu im Gegensatz zu YouTube von Anfang an auf seiner Plattform außer UGC-Videoclips in größerem Umfang auch professionelle Inhalte anbieten konnte, was maßgeblich zur Attraktivität dieses Dienstes bei den Nutzern beitrug, s.u. 7. Kapitel, Teil A.III.2.d.cc.

540 *Ohne Autor*, Soziale Netzwerke vor der Gewinnschwelle, Frankfurter Allgemeine Zeitung, 29.9.2009, S. 23.

541 *comScore*, 36 Million German Internet Users Viewed More Than 6 Billion Videos Online in August 2009, 27.10.2009, http://www.comscore.com/Press_Events/Press_Releases/2009/10/36_Million_German_Internet_Users_Viewed_More_Than_6_Billion_Videos_Online_in_August_2009 (zuletzt abgerufen am 01.07.2010).

542 Vgl. die Anleitung für die Nutzer zur Herstellung eines solchen *embedded video* unter http://www.google.com/support/youtube/bin/answer.py?hl=en&answer=57788 (zuletzt abgerufen am 01.07.2010).

543 Die Nutzungsbedingungen sind abrufbar unter http://www.youtube.com/t/terms (zuletzt abgerufen am 01.07.2010).

dieser Vorgabe von einem Nutzer auf die Webseite eingestellt werden, können von YouTube entfernt werden.[544] Zum Schutz ihrer Urheberrechte stellt YouTube Rechtsinhabern spezielle Hilfsmittel, sogenannte „copyright protection tools", zur Verfügung.[545] Zum einen können Rechtsinhaber YouTube über eine „copyright notice" über Urheberrechtsverletzungen informieren, was einer Benachrichtigung, wie sie das Notice&Takedown-Verfahren gemäß 17 U.S.C. § 512(c)(3) vorsieht,[546] entspricht. Insoweit bietet YouTube ein beschleunigtes internetbasiertes Verfahren an, bei dem die Rechtsinhaber die Benachrichtigung über ein auf der Webseite zur Verfügung gestelltes Formular unmittelbar an YouTube absenden können.[547] Zum anderen bietet YouTube ein Programm zur Inhaltsüberprüfung an, welches es Rechtsinhabern, deren Werke häufig Gegenstand von Urheberrechtsverletzungen sind, insbesondere ermöglicht, „Mehrfachentfernungen" anzufordern, d.h. nicht jede rechtswidrige Videodatei einzeln beanstanden zu müssen, sondern den Internetdienst in seiner Gesamtheit nach einem bestimmten Inhalt zu durchsuchen und überall dort, wo er aufgefunden wird, entfernen zu lassen.[548] Darüber hinaus stellt YouTube Rechtsinhabern eine Content-Identification-Technologie in Form von „YouTube Audio-ID" und „YouTube Video-ID" zur Verfügung, über die die Rechtsinhaber den Internetdienst nach bestimmten Multimediawerken durchsuchen lassen können.[549] Schließlich sehen die Nutzungsbedingungen eine „repeat infringers policy" vor, d.h. ein Verfahren zur Beendigung eines Nutzerkontos, wenn deren Inhaber wiederholt durch ein urheberrechtswidriges Verhalten auffällt.[550]

2. Soziale Netzwerke

a. Allgemein

Soziale Netzwerke sind Internetdienste, innerhalb deren die Darstellung der eigenen Person sowie die Vernetzung mit anderen Personen, mit denen sich ein Nutzer

544 Vgl. Ziff. 9.2 und 9.3 der Nutzungsbedingungen.
545 Vgl. den Überblick über *copyright protection tools* in der Rubrik „Content Management", abrufbar unter http://www.youtube.com/t/content_management (zuletzt abgerufen am 01.07.2010).
546 Vgl. 8. Kapitel, Teil B.III.4.f.
547 Vgl. die Beschreibung „Benachrichtigungen bei Urheberrechtsverletzungen, abrufbar unter http://www.youtube.com/t/copyright_notice (zuletzt abgerufen am 01.07.2010).
548 Vgl. die Beschreibung „Programm zur Inhaltsprüfung", abrufbar unter http://www.youtube.com/t/copyright_program (zuletzt abgerufen am 01.07.2010).
549 Vgl. die Beschreibung der Audio- und Video-ID-Technologie, abrufbar unter http://www.youtube.com/t/contentid (zuletzt abgerufen am 01.07.2010); vgl. 7. Kapitel, Teil B.II.3.
550 Vgl. Ziff. 7.2 der Nutzungsbedingungen.

durch einen gemeinsamen Nenner (wie beispielsweise einem Interesse am gleichen Musik- oder Filmgenre) verbunden sieht, im Vordergrund steht.[551] Der Nutzer kann im Rahmen dieser Angebote ein Profil erstellen, über das er bestimmte Informationen über seine Person öffentlich zugänglich macht. Die speziell „soziale" Komponente solcher Dienste besteht darin, dass der Nutzer auch bekanntgeben kann, mit welchen anderen Nutzern er im Rahmen des Internetdienstes vernetzt ist, auf die dann ein Besucher seines Profils wiederum zugreifen und sie, sofern diese seiner Kontaktanfrage zustimmen, seinen eigenen Kontakten hinzufügen kann. Auf diese Weise entstehen große soziale Netzwerke, in denen sich Personen mit gleichgelagerten Interessen oder bestimmten Berührungspunkten zusammenfinden und die sich durch das Hinzustoßen weiterer Nutzer und damit neuer Kontakte ständig erweitern.

b. Facebook, MySpace und die VZ-Netzwerke

Mit mehr als 300 Millionen Nutzern weltweit, davon ca. 6 Millionen allein in Deutschland, ist der Internetdienst Facebook gegenwärtig das populärste aller sozialen Netzwerke.[552] Der Internetdienst wurde im Jahr 2004 durch einige Studenten der Eliteuniversität Harvard gegründet und seine Nutzung ursprünglich auf die Studenten dieser Universität begrenzt. Später wurde der Nutzerkreis nach und nach erweitert, so dass nunmehr jeder, der das erforderliche Mindestalter von 13 Jahren erreicht hat, den Internetdienst nutzen kann. Im Rahmen der Plattform kann jeder Nutzer ein Profil über sich erstellen, einschließlich Fotos und einer Beschreibung seiner Hobbies, und mit anderen privat oder öffentlich Nachrichten austauschen, sowie Freunde zu Gruppen einladen und selbst Mitglied dieser Gruppen werden.

Ein weiteres, sehr populäres soziales Netzwerk ist der Internetdienst MySpace.[553] Dieser wurde im Jahr 2003 zu dem Zweck gegründet, Internetnutzern ein Portal zu bieten, auf dem sie sich auf der Grundlage gemeinsamer Interessen treffen können. Auch im Rahmen dieses Internetdienstes können die Nutzer ein Profil erstellen, indem sie sich selbst sowie ihre Interessen beschreiben. Dem Profil können auch Inhalte wie beispielsweise Videoclips oder Tonaufnahmen hinzugefügt werden. Über die „bulletin board"-Funktion kann ein Nutzer an alle seinem Profil als „Freunde" hinzugefügten Nutzer Nachrichten senden; weiterhin kann ein Nut-

551 Vgl. *Heckmann,* in: *Heckmann* (Hrsg.), jurisPK-Internetrecht, 2007, Kap. 1.7 Rn. 195.

552 http://www.facebook.com; *Ohne Autor*, Soziale Netzwerke vor der Gewinnschwelle, Frankfurter Allgemeine Zeitung, 29.9.2009, S. 23; vgl. den Eintrag im Weblog des Internetdienstes (abrufbar unter http://Weblog.facebook.com/Weblog.php (zuletzt abgerufen am 01.07.2010)) von *Mark Zuckerberg*, Vorstandsvorsitzender von Facebook, vom 15.09.2009.

553 http://www.myspace.com.

zer bestimmten Gruppen beitreten und mit einzelnen Nutzern „instant messages“ austauschen. Seit September 2009 betreibt die Plattform in Kooperation mit einigen Tonträgerunternehmen zudem den Musikdienst „MySpace Music“, der es seinen Nutzern ermöglicht, Tonaufnahmen als Streams in ihre Profile einzubetten sowie unmittelbar über die Plattform Musikdownloads zu erwerben.[554]

In Deutschland spielen im Bereich der sozialen Netzwerke vor allem die Plattformen des seit Anfang 2007 zur Verlagsgruppe Georg von Holtzbrinck gehörenden Unternehmens VZnet Netzwerke Ltd., die die Netzwerke studiVZ, schülerVZ und meinVZ („VZ-Netzwerke“) betreiben, eine große Rolle. Ende 2005 wurde zunächst das Portal studiVZ[555] für Studenten aus Deutschland, Österreich und der Schweiz gegründet. Darauf folgte 2007 das an Schüler gerichtete Netzwerk schülerVZ[556] und schließlich im Jahr 2008 das jedem Internetnutzer unabhängig von der Zugehörigkeit zu einer bestimmten Personengruppe offenstehende Netzwerk meinVZ.[557] Alle drei Plattformen bieten die klassischen Funktionen von sozialen Netzwerken: Erstellung eines Nutzerprofils, Möglichkeit der Suche nach bestimmten anderen Nutzern, Anzeige von Kontakten, Bildung von Gruppen und Hochladen von Inhalten im Rahmen der Profile. Im Oktober 2009 verzeichneten alle drei VZ-Netzwerke insgesamt 15,5 Millionen Mitglieder.[558]

III. Gefahren und Chancen des Web 2.0

Das Web 2.0 birgt sowohl Gefahren als auch Chancen für die Kommerzialisierung von urheberrechtlich geschützten Multimediawerken.

1. Gefahren

Durch die vielfachen neuen Möglichkeiten, die das Web 2.0 den Nutzern eröffnet, um digitale Inhalte zu bearbeiten, öffentlich zugänglich zu machen und zu verbreiten, erhöht sich gleichzeitig die Gefahr rechtsverletzender Handlungen in Be-

554 *Heise Online*, MySpace startet Musikdienst, 25.09.2008, http://www.heise.de/newsticker/meldung/116483 (zuletzt abgerufen am 01.07.2010).
555 http://www.studivz.net.
556 http://www.schuelervz.net.
557 http://www.meinvz.net.
558 Pressemitteilung des Unternehmens auf dem VZWeblog vom 16.10.2009, abrufbar unter http://Weblog.studivz.net/2009/10/16/meinvz-knackt-die-4-millionen-mitglieder-marke-vz-netzwerke-wachsen-damit-auf-rund-155-millionen-nutzer/ zuletzt abgerufen am 01.07.2010).

zug auf urheberrechtlich geschützte Multimediawerke.[559] So werden beispielsweise auf der Videoplattform YouTube zwar überwiegend selbstgedrehte Videoclips mit alltäglichen Erlebnissen und Episoden der Nutzer eingestellt, jedoch werden gerade auch im Rahmen solcher „home videos" gerne zur musikalischen Untermalung populäre Tonaufnahmen verwendet oder bestehen solche Videoclips oftmals aus einem Zusammenschnitt von Episoden aus bekannten Kino- oder TV-Filmen und -Serien. Bereits im Zusammenhang mit solchen Videoclips stellt sich die Frage nach deren urheberrechtlichen Zulässigkeit, wenn diese zwar nicht in Gänze, aber teilweise aus fremdem, urheberrechtlich geschütztem Material bestehen.[560] Hingegen bestehen keine Zweifel an der Urheberrechtswidrigkeit der großen Anzahl von Videoclips, Tonaufnahmen und Bildern, die Kopien urheberrechtlich geschützter Multimediawerke beinhalten und von den Nutzern im Rahmen von Web 2.0-Diensten hochgeladen werden, und die auf diese Weise ohne Erlaubnis der Rechtsinhaber der Öffentlichkeit in Teilen oder in Gänze zugänglich gemacht werden.

2. Chancen

a. Demokratisierung der Produktion und des Vertriebs von Multimediawerken

Durch die ubiquitäre Verfügbarkeit von internetbasierten Technologien und Plattformen zur Herstellung von multimedialen Inhalten in Kombination mit sinkenden Kosten für immer schnellere Internetverbindungen verringern sich die Produktionskosten und damit die Hindernisse für den Eintritt neuer Wettbewerber in den Markt für Multimediawerke.[561] Das Internet wird zunehmend zu einem wichtigen Faktor bei der Herstellung und dem Vertrieb von Multimediawerken. Auch erhöht sich die Anzahl von Personen und Unternehmen, die an diesen Prozessen beteiligt sind. Der Herstellungsprozess von Multimediawerken wird somit „demokratisiert", da nunmehr auch ein durchschnittlicher Nutzer des Internets und nicht nur ein mit erheblichen finanziellen Mitteln ausgestattetes Medienunternehmen am Wettbe-

559 *Meyers*, 26 Cardozo Arts & Entertainment L. J. 935, 936 (2009); *Montagnani*, 26 Cardozo Arts & Ent. L.J. 719, S. 769 (2009).

560 Fraglich ist die Zulässigkeit vor allem nach U.S.-amerikanischem Urheberrecht, da demnach die Fair-Use-Doktrin eine gewisse Grauzone eröffnet, in deren Rahmen die Nutzung urheberrechtlich geschützten Materials zulässig sein kann, wenn die Nutzung sich in gewissen Grenzen hält, selbst keine kommerziellen Zwecke verfolgt und den Markt des genutzten urheberrechtlich geschützten Werks nicht beeinträchtigt.

561 *OECD*, Web 2.0, 2007, S. 28.

werb hinsichtlich der Vermarktung und des Vertriebs von Multimediawerken teilnehmen kann.[562]

b. Revolutionierung der Kommunikationswege und des Austauschs von Informationen

Weiterhin werden durch das Web 2.0 die traditionellen Kommunikationswege und damit die zwischen Einzelpersonen bestehenden sozialen Kontakte in ihrer Entstehung und in ihren Abläufen revolutioniert.[563] Denn im Rahmen von sozialen Netzwerken kann ein Nutzer mit einer Vielzahl von Personen in Kontakt treten, die zuvor für ihn aufgrund einer räumlichen Entfernung oder aus anderen Gründen unerreichbar gewesen wären. Damit erhält er gleichzeitig Zugang zu einer Fülle neuer Informationen, Ideen und Kenntnisse, die wiederum seinen eigenen Informationsstand und seine Interessen beeinflussen können. Aufgrund dieses erweiterten Informationsflusses können Web 2.0-Dienste somit dazu beitragen, den politischen und gesellschaftlichen Diskurs zu bereichern und die Informationsfreiheit sowie die freie Meinungsäußerung zu befördern.[564] Diese Veränderungen in der Art und Weise, wie Nutzer Informationen und Know-How austauschen, haben das Potenzial, zu einer größeren Unabhängigkeit der Nutzer zu führen und ihre Teilhabe am Austausch von Informationen zu erhöhen.[565]

c. Das Web 2.0 als wesentliches Marketinginstrument

Weiterhin stellen Web 2.0-Dienste gerade im Musikbereich für Künstler und Bands, die bisher noch weitgehend unbekannt sind, ein äußerst hilfreiches Werkzeug dar, um sich hierüber zu vermarkten, d.h. ihren Bekanntheitsgrad und damit die Chancen auf einen Vertrag mit einem Tonträgerunternehmen zu erhöhen.[566] So spielt beispielsweise das Videoportal YouTube nicht nur für unabhängige Künstler, sondern auch für Tonträgerunternehmen eine zentrale Rolle in ihrer Marketingstrategie, da dieser Internetdienst sich zu einem Dreh- und Angelpunkt für neue Musikangebote entwickelt hat, die um die Aufmerksamkeit interessierter Musik-

562 *OECD*, Web 2.0, 2007, S. 12: *„The Internet as a new creative outlet has altered the economics of information production, increased the democratisation of media production and led to changes in the nature of communication social relationships (sometimes referred ot as the „rise – or return – of the amateurs)“.*
563 *OECD*, Web 2.0, 2007, S. 12.
564 *OECD*, Web 2.0, 2007, S. 12.
565 *OECD*, Web 2.0, 2007, S. 12.
566 *Einhorn*, Gorillas in Our Midst, 2007, S. 16-17.

fans konkurrieren.[567] Aus diesem Grund haben fast alle großen Tonträgerunternehmen mit YouTube und anderen, ähnlich musikaffinen Internetdiensten wie beispielsweise MySpace[568] Music oder imeem entsprechende Lizenzvereinbarungen getroffen, wonach urheberrechtlich geschützte Tonaufnahmen samt der zugehörigen Musikvideos der bei diesen Unternehmen unter Vertrag stehenden Künstler auf diesen Internetdiensten öffentlich zugänglich gemacht werden dürfen.[569]

Darüber hinaus bringen Web 2.0-Dienste eine neue Generation von hauptsächlich im Internet aktiven, von den Tonträgerunternehmen unabhängigen Musikkritikern hervor, die ihre Empfehlungen an die Nutzer über News-Dienste und Weblogs und damit über Wege verbreiten, die von den Tonträgerunternehmen kaum kontrollierbar sind.[570] Dies stellt eine entscheidende Veränderung im Vermarktungsprozess von Musikprodukten dar, der bisher vorwiegend durch die Tonträgerunternehmen gesteuert wurde, beispielsweise indem Radiostationen für das Abspielen neuer Tonaufnahmen in ihren Programmen bezahlt wurden oder Künstler mit ihren neuen Musikalben in bestimmten Fernsehsendungen mit hoher Popularität platziert wurden.[571]

d. Kommerzialisierungspotential der werbefinanzierten Geschäftsmodelle des Web 2.0

Sowohl in der Musik- als auch in der Filmindustrie zeichnet sich ein Trend ab, wonach urheberrechtlich geschützte Multimediawerke den Nutzern im Rahmen von Web 2.0-Diensten zunehmend kostenlos zur Verfügung gestellt und diese Angebote mittels der Zuschaltung von Werbebotschaften zu dem jeweils vom Nutzer konsumierten Multimediawerk finanziert werden (sogenannte „werbebasierte Geschäftsmodelle“ oder „ad-supported business models“).[572] Da erwartet wird, dass die Ausgaben für Internetwerbung in den nächsten Jahren erheblich steigen und

567 Vgl. hierzu *Reinke*, Wertschöpfungsmöglichkeiten Musikindustrie, 2009, S. 81.
568 *Bernstein/Sekine/Weissman*, Global Music Industry, 2007, S. 29.
569 Zum Zeitpunkt des Abschlusses dieser Arbeit bestanden seitens YouTube wirksame Vereinbarungen mit Universal Music Group, Sony Music Entertainment und EMI; mit Warner Music wurde noch über eine Erneuerung der inzwischen ausgelaufenen Lizenzvereinbarungen verhandelt, vgl. *Sandoval*, YouTube, Warner Music feud nearing an end, CNET News, 18.09.2009, http://news.cnet.com/8301-1023_3-10356764-93.html (zuletzt abgerufen am 01.07.2010); *ohne Autor*, YouTube darf wieder Warner-Videos zeigen, 30.09.2009, tagesschau.de, http://www.tagesschau.de/warnertube100.html (zuletzt abgerufen am 01.07.2010).
570 *Einhorn*, 56 J. Copyright Soc’y, 201, 207 (2008).
571 In Deutschland wird zu diesem Zweck seit Jahrzehnten die Unterhaltungsshow „Wetten dass...“ genutzt, vgl. *Schulz*, Schluss mit lustig, Spiegel Online, 05.02.2005, http://www.spiegel.de/spiegel/print/d-39257707.html (zuletzt abgerufen am 01.07.2010).
572 *Montagnani*, 26 Cardozo Arts & Ent. L.J. 719, 764 (2009).

die Ausgaben für tradierte (offline) Marketingkonzepte übertreffen und teilweise ersetzen werden,[573] steht dieser Ansatz zur Kommerzialisierung von Multimediawerken derzeit im Zentrum der Diskussionen über die Zukunft der Multimediaindustrie.

aa. Grundlagen werbefinanzierter Geschäftsmodelle

Eines der ersten Unternehmen, das im Musikbereich mit einem werbefinanzierten Geschäftsmodell experimentierte, war der Suchmaschinenanbieter Yahoo. Dem Unternehmen gelang es, auf der Grundlage der Zuschaltung von Werbebotschaften kostenlos einen Internetdienst mit einem herausragenden Katalog an Musikvideos und Webcasts von über 200 Internetradiosendern anzubieten,[574] der sich innerhalb kürzester Zeit zu einem der am meisten besuchten Internetplattformen entwickelte.[575] Damit ging die Rechnung des Unternehmens auf, durch attraktive Inhalte mehr und mehr Nutzer anzulocken, die es über die zugeschalteten Werbebotschaften an seine Werbepartner weitervermitteln konnte.

Werbefinanzierte Geschäftsmodelle basieren darauf, einen „virtuellen Kreislauf" in Gang zu setzen, in dessen Verlauf sich die Qualität des jeweiligen Internetdienstes beständig dadurch erhöht, dass sich durch wachsende Nutzerzahlen die Funktionen des Internetdienstes verbessern (beispielsweise da hierdurch mehr Inhalte auf den Internetdienst gelangen oder sich die Netzwerkeffekte durch eine immer höhere Anzahl an Nutzern verstärken), wodurch wiederum mehr Nutzer von dem Dienst angezogen werden. Als Folge hieraus steigt die Bereitschaft der Anbieter von Inhalten, diese auf dem Dienst zur Verfügung zu stellen, um hierdurch von der zunehmender Popularität des Dienstes und den daraus resultierenden Vertriebs und Vermarktungseffekten zu profitieren, was die Attraktivität des Dienstes weiter steigert.[576] Aufgrund der wachsenden Nutzerzahlen wird der Dienst auch für Werbepartner immer attraktiver, wodurch schließlich auch der wirtschaftliche Wert des Internetdienstes wächst.[577]

573 Angeblich werden die Ausgaben für Internetwerbung in den USA bis 2011 auf insgesamt 27,2 Mrd. Dollar steigen, von 8,6 Mrd. Dollar im Jahr 2007, vgl. *Montagnani*, 26 Cardozo Arts & Ent. L.J. 719, 768 (2009); s.a. *Einhorn*, Gorillas in Our Midst, 2007, S. 16.
574 http://new.music.yahoo.com/.
575 *Einhorn*, 56 J. Copyright Soc'y, 201, 204 (2008).
576 *Einhorn*, 56 J. Copyright Soc'y, 201, 205 (2008).
577 *Einhorn*, 56 J. Copyright Soc'y, 201, 204 (2008).

bb. Rückbesinnung auf werbefinanzierte Geschäftsmodelle nach den Misserfolgen des Einsatzes von DRM-Systemen bei Musikdownloads

Da man in der Musikindustrie bis vor kurzem davon ausging, die Kontrolle über die Verbreitung von digitalen Multimediawerken durch den Einsatz von DRM-Systemen wiedererlangen zu können und die Filmindustrie diesen Glauben weiterhin zu pflegen scheint,[578] wurden *ad-supported business models* lange Zeit vernachlässigt. Da der Erfolg von DRM-gestützten Geschäftsmodellen sowohl im Musik- als auch im Filmbereich jedoch zumindest hinter den Erwartungen der Multimediaindustrie zurückgeblieben ist und zudem die massenhafte Verbreitung illegaler Filesharing-Netzwerke faktisch zu einer ubiquitären, kostenlosen Verfügbarkeit von Multimediawerken geführt hat, begann man sich in den letzten Jahren auf diesen Ansatz zurückzubesinnen.[579] Denn die Stärke werbefinanzierter Geschäftsmodelle liegt darin, dass hierüber den Nutzern Multimediawerke kostenlos angeboten werden können, weswegen sie eine ernsthafte Konkurrenz für illegale Angebote darstellen. Dennoch erhalten die Rechtsinhaber eine Kompensation für die Nutzung ihrer Werke in Form eines Anteils aus den Einnahmen aus dem Verkauf von Werbeflächen.[580]

578 Vgl. 5. Kapitel, Teil E.

579 *Montagnani*, 26 Cardozo Arts & Ent. L.J. 719, S. 765 (2009).

580 *IFPI*, Digital Music Report 2008, S. 15: *„Advertising-supported music services are a small but potentially significant revenue stream for record companies, which some see as the logical strategy for reclaiming a younger generation of consumers habituated to a culture of "free" music. According to Jupiter Research file-sharing currently dominates music acquisition among younger consumers. In 2007 over a third (34 per cent) of internet users aged 15–24 illegally file-shared music. This is three times the rate of legal service usage among this age group. Ad-supported services offer consumers free access to streamed or downloaded music while artists and record companies are compensated by revenues generated by advertising. The best examples of this are the recent deals between some record companies and social networks such as MySpace, Bebo, YouTube, LastFM and Imeem. These deals are mostly based on licensing agreements for streaming music and music videos for a share of advertising revenues. Questions remain however as to the potential for ad-supported models as some believe the addition of ads on free services will divert consumers elsewhere, and there are continuing concerns over copyright infringement. So far the model has worked best in growing the video-on-demand business. Progress was made in 2007 to create a global rights body to act as a centralised licensing service for independent record companies whose music is used on sites such as YouTube and who wish to negotiate deals with services. The body is known as Merlin and runs as a sister organisation to the global independent record labels body WIN."*; s.a. *OECD*, Web 2.0, 2007, S. 49; *Krasilovsky/Shemel*, Music Business, 2007, S. 444 f.

cc. Unsicherheiten betreffend die Wirtschaftlichkeit von werbebasierten Geschäftsmodellen

Allerdings wurden werbefinanzierte Geschäftsmodelle von der Multimediaindustrie auch deswegen lange Zeit vernachlässigt, da man befürchtete, mit den damit zu erzielenden Werbeeinnahmen den Ausfall der Einnahmen aus dem Vertrieb von physischen Datenträger nicht kompensieren zu können. Die Wirtschaftlichkeit von werbefinanzierten Geschäftsmodellen ist nach wie vor umstritten.[581]

(1) Indizien für die Wirtschaftlichkeit von werbebasierten Geschäftsmodellen

Mittlerweile mehren sich jedoch die Anzeichen dafür, dass es Unternehmen durchaus möglich ist, auf der Basis eines rein werbefinanzierten Geschäftsmodells in die Gewinnzone vorzustoßen.

So teilte beispielsweise das soziale Netzwerk Facebook im September 2009 mit, dass es fünf Jahre nach seiner Gründung und Investitionen in Höhe von insgesamt US$ 700 Millionen im zweiten Quartal 2009 erstmals einen positiven Mittelzufluss erreicht habe[582] und dass es weiterhin erwarte, im Jahr 2009 insgesamt US$ 500 Millionen umzusetzen.[583] Hierbei dürfte eine wesentliche Rolle spielen, dass inzwischen bereits 80 der 100 größten US-Unternehmen Facebook zu Werbezwecken nutzen und das soziale Netzwerk daher entsprechende Werbeeinnahmen verzeichnen kann.[584] Ebenso ließ die deutsche VZnet-Gruppe[585] verlauten, dass die Erwirtschaftung eines Gewinns für sie in greifbare Nähe gerückt sei, da man in einigen Monaten des Jahres 2009 bereits Gewinne erzielt habe, auch wenn man über das Gesamtjahr gerechnet noch in der Verlustzone bleibe.[586]

Auch nach Angaben des Marktführers im Bereich Videoplattformen YouTube nehmen die Umsätze aufgrund der Zuschaltung von Werbebotschaften zu urheberrechtlich geschützten Multimediawerken im Vergleich zu den Anfangsjahren des Internetdienstes gegenwärtig massiv zu.[587] Praktisch bedeutet diese Entwick-

581 *OECD*, Web 2.0, 2007, S. 50; *Einhorn*, 56 J. Copyright Soc'y, 201, 206 (2008).
582 Vgl. den Eintrag im Weblog des Internetdienstes (abrufbar unter http://Weblog.facebook.com/Weblog.php (zuletzt abgerufen am 01.07.2010)) von *Mark Zuckerberg*, Vorstandsvorsitzender von Facebook, vom 15.09.2009.
583 *Ohne Autor*, Soziale Netzwerke vor der Gewinnschwelle, Frankfurter Allgemeine Zeitung, 29.9.2009, S. 23.
584 *Ohne Autor*, s.o.
585 Vgl. 7. Kapitel, Teil A.II.2.b.
586 *Ohne Autor*, Soziale Netzwerke vor der Gewinnschwelle, Frankfurter Allgemeine Zeitung, 29.9.2009, S. 23.
587 *Sandoval*, Universal digital chief on iTunes, DRM, and Android, CNET News, 12.01.2009, http://news.cnet.com/8301-1023_3-10140244-93.html?part=rss&tag=feed&subj=News-DigitalMedia (zuletzt abgerufen am 01.07.2010).

lung, dass beispielsweise das Unternehmen Universal aufgrund seiner Kooperation mit Web 2.0-Diensten in Bezug auf Tonaufnahmen und Musikvideos, an denen Universal Rechte hält, für das Jahr 2009 einen Jahresumsatz im zweistelligen Millionenbereich erzielt hat.[588] Konkret werden die Einnahmen, die Universal durch Streaming-Angebote auf Internetdiensten wie YouTube, MTV und MySpace insgesamt erzielt hat, auf etwa US$ 100 Millionen geschätzt, wobei der Löwenanteil auf die Kooperation mit YouTube entfallen dürfte.[589]

Weiterhin kommt webefinanzierten Geschäftsmodellen im Zusammenhang mit Web 2.0-Diensten, die den Konsum von Multimediawerken über das Internet anbieten, der Trend entgegen, dass seitens der Nutzer die Nachfrage nach sogenanntem „long-form content", d.h. nach TV-Filmen und Shows, die länger als 20 Minuten dauern, steigt. Damit erhöht sich jedoch gleichzeitig die Attraktivität von Internetdiensten, die solchen *long-form content* anbieten. So liegt beispielsweise in den USA der Anteil derjenigen Internetnutzer, die solche Angebote mindestens einmal im Monat nutzen, mittlerweile bei 26 Prozent und sogar bei 51 Prozent in der Gruppe der 18- bis 24-Jährigen.[590] Dieser Trend zeigt sich auch am steigenden Anteil von sogenannter „Echtzeit-Unterhaltung", d.h. dem Abruf von Video- und Audiostreams, wie sie in der Regel im Rahmen Web 2.0-Diensten angeboten werden, am weltweiten Internetverkehr. So hat sich dieser Anteil 2009 auf 27 Prozent erhöht und damit im Vergleich zum Vorjahr um 14 Prozent zugenommen,[591] woran deutlich wird, dass diese Angebote mittlerweile einen wichtigen Faktor bei der täglichen Nutzung des Internets darstellen.

588 *Sandoval*, s.o.

589 *Sandoval*, Universal Music seeing 'tens of millions' from YouTube, CNET News, 18.12.2008, http://news.cnet.com/8301-1023_3-10126439-93.html?tag=mncol;txt (zuletzt abgerufen am 01.07.2010). Die Frage, in welchem Umfang YouTube selbst an der Verbindung von den auf seiner Plattform vorhandenen Videos mit Werbung verdient, ist jedoch trotz solcher Erfolgsmeldungen Gegenstand heftiger Spekulationen, vor allem da das Unternehmen insoweit keinerlei Zahlen veröffentlicht und Stellungnahmen dazu weitgehend ablehnt. Dementsprechend weit lagen die Schätzungen des für das Unternehmen in den USA im Jahr 2009 zu erwartenden Jahresumsatzes auseinander, und reichten von einem Umsatzplus von US$ 100 (Medienanalysten von Screen Digest) bzw. US$ 500 (Jefferies & Co.) Millionen Dollar bis hin zu einem Verlust in Höhe von US$ 470 Millionen Dollar (Credit Suisse); vgl. hierzu auch *Dignan*, Google moves to show YouTube has „a very credible business model", ZDNet, 17.07.2009, http://blogs.zdnet.com/BTL/?p=21288 (zuletzt abgerufen am 01.07.2010).

590 *Anderson*, On demand in command: 51% of young Net users view TV online, Ars Technica, 06.08.2009, http://arstechnica.com/media/news/2009/08/half-of-all-young-internet-users-now-watch-tv-online.ars (zuletzt abgerufen am 01.07.2010).

591 *Heise Online*, Studie: Echtzeit-Unterhaltung ist Web-Traffic-Größe Nummer 1, 26.10.2009, http://www.heise.de/newsticker/meldung/Studie-Echtzeit-Unterhaltung-ist-Web-Traffic-Groesse-Nummer-1-839567.html (zuletzt abgerufen am 01.07.2010).

(2) Wesentlicher Erfolgsfaktor 1: Erhöhung der Attraktivität der Inhalte auf Web 2.0-Dienten für die Nutzer

Letztendlich dürfte entscheidend für den Erfolg oder Misserfolg von werbefinanzierten Web 2.0-Diensten sein, dass die im Rahmen eines solchen Internetdienstes angebotenen Inhalte für die Einbettung von Werbebotschaften ausreichend attraktiv werden.

Dieser Aspekt war in der Vergangenheit vor allem im Zusammenhang mit Videoplattformen problematisch, da die dort eingestellten Videoclips anfänglich vorwiegend aus echten nutzergenerierten Inhalte bestanden, bei denen die zumeist etwas eigenwilligen Inhalte[592] nur schwer mit professionellen Werbebotschaften von Unternehmen zu verbinden waren.[593] Nunmehr sind jedoch auf Videoplattformen zunehmend auch professionelle Inhalte vorhanden, wodurch die Attraktivität für Werbepartner steigt. Auf dem Videoportal Hulu beispielsweise sind anstatt nutzergenerierter Inhalte Multimediawerke, die von etablierten Medienunternehmen wie NBC Universal, News Corp. oder Disneys ABC Enterprises produziert wurden, in voller Länge über einen qualitativ hochwertigen Video-Player abrufbar. Dementsprechend waren auch die von diesem Internetdienst angebotenen Werbeplätze innerhalb eines Monats nach der Bekanntmachung seiner Geschäftsaufnahme ausverkauft.[594] Aufgrund der Attraktivität seiner Inhalte ist Hulu innerhalb kurzer Zeit eine echte Konkurrenz für den Marktführer YouTube geworden, das für die Nutzer zudem eine ernstzunehmende Alternative zu illegalen Angeboten darstellt.[595]

Auch bei YouTube hat sich die Anzahl von umsatzrelevanten, d.h. zur Verbindung mit Werbebotschaften geeigneten Videoclips gesteigert, so dass sich der Abruf „werberelevanter" Inhalte durch die Nutzer auf dem Internetdienst innerhalb eines Jahres von ca. 3 auf 9 Prozent verdreifacht hat.[596] Zudem nutzen nach Angaben von YouTube nunmehr mehr als 70 Prozent aller „Ad Age Top 100" Mar-

592 Wie beispielsweise Aufnahmen von Haustieren oder Familienmitgliedern.

593 *McCarthy*, MTV Networks: which video ads work best, CNET News, 15.07.2009, http://news.cnet.com/8301-1023_3-110287132-93.html?part=rss&tag=feed&subj=News-DigitalMedia (zuletzt abgerufen am 01.07.2010).

594 *McCarthy*, s.o.

595 So *Garland* (s.o. Fn. 500) zitiert bei *Sandoval*, End of the world as Hollywood knows it, CNET News, 20.10.2009, http://news.cnet.com/8301-31001_3-10378654-261.html (zuletzt abgerufen am 01.07.2010): *„What you have is a very effective antipiracy tool in Hulu, and I'm specifically drawing on numbers and not just citing anecdotal evidence. People really do prefer the Hulu experience. ... You have a legitimate market stealing share and audience away from a pirate market."*.

596 *Dale/Zamost*, YouTube myth busting, YouTube Biz Weblog, 20.07.2009, http://ytbizblog.blogspot.com/2009/07/youtube-myth-busting.html (zuletzt abgerufen am 01.07.2010); *Krazit*, YouTube slowly building ad-friendly content, CNET News, 08.05.2009, http://news.cnet.com/8301-1023_3-10236753-93.html?part=rss&tag=feed&subj=News-DigitalMedia (zuletzt abgerufen am 01.07.2010).

ketingfirmen die Videoplattform im Zusammenhang mit ihren Werbekampagnen.[597] Generell scheinen die Bedenken der Werber gegen die Werbewirksamkeit von Web 2.0-Diensten abzunehmen, da einer Umfrage des Marktforschungsunternehmens Emarketer zufolge 75 Prozent der befragten amerikanischen Werber vorhat, im kommenden Jahr die Ausgaben vor allem in sozialen Netzwerken zu erhöhen. Damit genießen diese Internetdienste bei den Werbepartnern Priorität noch vor Suchmaschinen und verweisen herkömmliche Medien wie beispielsweise Zeitungen auf die hinteren Plätze.[598]

(3) Wesentlicher Erfolgsfaktor 2: Erhöhung der Konversionsrate

Die abschließende Beurteilung der Erfolgsaussichten werbefinanzierter Geschäftsmodelle bleibt jedoch vor allem auch deswegen schwierig, weil deren Erfolg unter anderem auch von der Neu- und Fortentwicklung von Technologien abhängt, die es ermöglichen, sowohl das Angebot des jeweiligen Internetdienstes als auch die in diesem Zusammenhang zugeschalteten Werbebotschaften besser auf den individuellen Nutzer abzustimmen.[599] Eine solche verfeinerte Abstimmung ist Voraussetzung für die Erhöhung der „Konversionsrate", mit der die Wirksamkeit von Werbebotschaften gemessen wird. Demnach zeigt sich die Effektivität von Werbemaßnahmen an der Höhe des Anteils der Nutzer, der aufgrund einer ihnen angezeigten Werbebotschaft das darin angebotene Produkt oder die darin beworbenen Dienstleistung tatsächlich erwirbt. Kann diese Rate erhöht werden, so steigt damit für den Werbepartner der Wert des einzelnen Nutzers und damit gleichzeitig des Internetdienstes, zu dessen Kundenstamm diese Nutzer gehören.[600]

597 *Dale/Zamost*, YouTube myth busting, YouTube Biz Weblog, 20.07.2009, http://ytbiz-blog.blogspot.com/2009/07/youtube-myth-busting.html (zuletzt abgerufen am 01.07.2010).^^^^ Diese Entwicklung dürfte dadurch begünstigt worden sein, dass YouTube seinen Kooperationspartnern seit einiger Zeit erlaubt, die ihnen im Rahmen der Videoplattform im Zusammenhang mit ihren Inhalten zur Verfügung gestellten Werbeplätze selbst zu verkaufen. Damit werden die Unternehmen in die Lage versetzt, die Preise, die sie regelmäßig für die Zuschaltung von Werbung zu ihren Inhalten verlangen können und die oftmals höher liegen als diejenigen, die Google am Werbemarkt einzuwerben in der Lage ist, auf die auf der Plattform verfügbaren Werbekapazitäten zu übertragen; vgl. *Sandoval*, Could peace be near for YouTube and Hollywood?, CNET News, 23.07.2008, http://news.cnet.com/8301-1023_3-9996905-93.html (zuletzt abgerufen am 01.07.2010).

598 *Ohne Autor*, Soziale Netzwerke vor der Gewinnschwelle, Frankfurter Allgemeine Zeitung, 29.9.2009, S. 23.

599 *OECD*, Web 2.0, 2007, S. 50; *Einhorn*, 56 J. Copyright Soc'y, 201, 206 (2008).

600 *Einhorn*, 56 J. Copyright Soc'y, 201, 207 (2008).

B. Technische Grundlagen und Anbieter von Content-Identification-Technologien

Content-Identification-Technologien basieren darauf, digitale Multimediawerke anhand von Merkmalen zu identifizieren, die Rückschlüsse auf deren sinnlich wahrnehmbaren Inhalt ermöglichen. Die hierzu eingesetzten sogenannten „perceptual hash functions" wurden auf der Grundlage von Technologien aus dem Bereich der Kryptographie entwickelt.

I. Cryptographic Hash Functions

„Digital Fingerprinting" ist eine andere Bezeichnung für die „cryptographic hash function", die aus dem Bereich der Kryptographie stammt. Diese wird beispielsweise zusammen mit *public-key*-Algorithmen zur Verschlüsselung von Daten und digitalen Signaturen sowie im Bereich der Integritäts- und Authentizitätskontrolle eingesetzt.[601] Die Funktion steht für einen Transformationsvorgang in Bezug auf einen Eingabewert (beispielsweise eine digitale Nachricht oder ein digitales Dokument), nach dessen Durchführung der Eingabewert in Form eines „fixed-size bit string" wiedergegeben wird, der auch als „hash value" oder „digitaler Fingerabdruck" bezeichnet wird.[602] Die beiden am weitesten verbreiteten *cryptographic hash functions* sind die von Ron Rivest 1992 erfundene sogenannte „MD5"[603]-Funktion, sowie die „SHA-1"[604]-Funktion, die 1993 von der US-amerikanischen National Security Agency veröffentlicht wurde.[605]

601 Vgl. 4. Kapitel, Teil B.II.1; *Schneier*, Cryptanalysis of MD5 and SHA: Time for a New Standard, Computerworld, 19.08.2004, http://schneier.com/essay-074.html (zuletzt abgerufen am 01.07.2010).

602 Vgl. *Wikipedia*, Stichwort „cryptographic hash function", Version vom 29.04.2010, 21:37 h, http://en.*Wikipedia*.org/w/index.php?title=Cryptographic_hash_function&oldid=359138309 (zuletzt abgerufen am 01.07.2010).

603 Akronym für „Message Digest 5".

604 Akronym für „Secure Hash Algorithm 1".

605 Im Jahr 2004 wurden bei beiden Funktionen Sicherheitslücken entdeckt, woraufhin das US-amerikanische National Institute of Science and Technology im Jahr 2007 das „cryptographic hash project" ausrief mit dem Ziel, anhand eines Wettbewerbs zwischen innovativen Hash-Algorithmen die Grundlage für eine neue, sicherere sogenannte „New Cryptographic Hash Algorithm (SHA-3) Family" zu schaffen; vgl. die Ankündigung des Projekts auf der Webseite der NIST, abrufbar unter http://csrc.nist.gov/groups/ST/hash/ (zuletzt abgerufen am 01.07.2010).

Cryptographic hash functions sind grundsätzlich hochsensibel für geringste Abweichungen der digitalen Zusammensetzung des jeweiligen Eingabewerts. Dies bedeutet, dass sich ein völlig anderer *hash value* ergibt, wenn am ursprünglichen Eingabewert auch nur ein einziges Bit abgeändert wird. Dies bedeutet jedoch auch, dass die Identifizierung eines Eingabewerts durch eine *cryptographic hash function* bereits dann fehlschlägt, wenn nur eine geringfügige Veränderung an der betroffenen Datei vorgenommen wurde, die so minimal sein kann, dass sie sich nicht in einer Veränderung des sinnlich wahrnehmbaren Inhalts der Datei niederschlägt.[606] Daher sind herkömmliche *crpytographic hash functions* für die Identifikation von digitalen Multimediawerken ungeeignet. Denn insoweit spielt gerade nicht das Format, die Kompression oder die Bitanzahl einer Datei, die ein digitales Multimediawerk enthält, die entscheidende Rolle, sondern vielmehr deren sinnlich wahrnehmbarer Inhalt.

Daher basieren die im Multimediabereich eingesetzten Content-Identification-Technologien auf „perceptual hash functions“[607] und damit auf einem digitalen Fingerabdruck, der eigens auf Medieninhalte abgestimmt ist. *Perceptual hash functions* folgen ebenso wie *crpytographic hash functions* dem Prinzip, dass unterschiedliche Eingabewerte (hier: unterschiedliche digitale Multimediawerke) unterschiedliche *hash values* generieren müssen. Jedoch sind für die Verschiedenheit der zu errechnenden Werte nicht rein technisch-formale Unterschiede wie Bitanzahl oder Dateiformat maßgeblich, sondern allein die Unterschiede im sinnlich wahrnehmbaren Inhalt der in den Dateien verkörperten Multimediawerke. Eine *perceptual hash function* stützt sich im Rahmen des durchgeführten Transformationsvorgangs zur Errechnung des *hash value* daher auf Merkmale wie Akustik, Farben und Bewegungen. Die spezielle Funktionsweise und Stärke von Content-Identification-Technologien besteht somit im Ergebnis darin, dass sie digitale Multimediawerke anhand ihrer sinnlich wahrnehmbaren, charakteristischen Ton- und Bildsignale identifizieren können.[608] Hierdurch sind Content-Identification-Technologien in der Lage, ein Multimediawerk auch dann wiederzuerkennen, wenn die das Werk enthaltende Datei verändert, komprimiert, konvertiert, neu aufgenommen oder an ihr anderweitige Manipulationen vorgenommen wurden. Denn solche

606 *Evans*, Perceptual Image Hashing: Methods, Image Hashing Research, University of Texas in Austin, http://users.ece.utexas.edu/~bevans/projects/hashing/methods.html (zuletzt abgerufen am 01.07.2010).

607 Vgl. die Beschreibung des “Perceptual Hashing”-Projekts der Polytechnic University, Information Systems and Internet Security Lab, http://isis.poly.edu/projects/percephash (zuletzt abgerufen am 01.07.2010).

608 *Herre*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 93; vgl. auch die Ausführungen zu der als „Fuzzy Hashing“ betitelten Technologie bei *Haber/Horne/Pato/Sander/Tarjan*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 224, 229.

Modifikationen lassen regelmäßig den charakteristischen, sinnlich wahrnehmbaren Inhalt des Multimediawerks unangetastet.[609] Anders ausgedrückt ist eine funktionierende Content-Identification-Technologie dazu in der Lage, ein multimediales Werk auch trotz etwaiger Manipulationen solange wiederzuerkennen, wie auch ein menschlicher Rezipient, der das digitale Multimediawerk ansieht oder anhört, in der Lage wäre, darin das originäre Werk wiederzuerkennen.[610] Anders als beispielsweise beim Einsatz von Wasserzeichentechnologien werden im Zusammenhang mit Content-Identification-Technologien dem jeweiligen digitalen Werk somit auch keine Informationen zum Zwecke der Identifikation hinzugefügt, sondern die Identität des jeweiligen multimedialen Inhalts unmittelbar aufgrund einer Analyse von dessen besonderen Eigenschaften, wie sie in den entsprechenden Ton- oder Bildsignalen zum Ausdruck kommen, ermittelt.[611]

609 *Bechtold*, DRM, 2002, S. 92. Ein Nutzer möchte über einen Web 2.0.-Dienst in der Regel anderen Nutzern den Konsum eines bekannten, urheberrechtlich geschützten Werks ermöglichen; dieses Ziel wird jedoch nicht erreicht, wenn die digitale Version dieses Werks so stark modifiziert wird, dass die anderen Nutzer das ursprünliche Werk nicht mehr wiedererkennen können. Daher müssen solche Modifikationen den wahrnehmbaren "Kern" des Multimediawerks weitgehend unangetastet lassen; es ist jedoch gerade dieser Kern, auf den sich Content-Identification-Technologien bei der Identifikation von digitalen Inhalten konzentrieren.

610 Solange somit ein menschlicher Hörer in der Lage wäre, eine Tonaufnahme wiederzuerkennen, obwohl an den Tonhöhen oder der Geschwindigkeit der Tonfolge dieser digitalen Tonaufnahme manipuliert wurde, kann auch eine Content-Identification-Technologie den Titel identifizieren.

611 Sogenannter „non-invasive approach". Der Prozess der Datenanalyse durchläuft zwei Stadien, die sogenannte „training"- und die „recognition"-Phase. In der *training phase* werden die charakteristische Besonderheiten, die das zu analysierende Multimediawerk in Bezug auf bestimmte Ton- oder Bildmerkmale – wie beispielsweise Tonspektrum und zeitliche Abfolge der einzelnen Töne bei einer Tonaufnahme bzw. Farbe, Form und Bewegung innerhalb der einzelnen Bilder bei einem Filmwerk – aufweist, durch eine Software extrahiert und auf diese Weise eine einzigartige Kombination an Referenzdaten geschaffen, anhand derer das Multimediawerk von allen anderen unterschieden werden kann. Dabei werden nur diejenigen Merkmale berücksichtigt, die von menschlichen Rezipienten sinnlich wahrgenommen werden, um auf diese Weise das Datenvolumen des Fingerabdrucks des Multimediawerks möglichst gering zu halten. Dieser Fingerabdruck, dessen Datenvolumen im Vergleich mit demjenigen der analysierten Datei, beispielsweise einer Tonaufnahme im MP3-Format, extrem komprimiert ist, wird sodann zusammen mit einigen den Inhalt beschreibenden Metadaten (beispielsweise Werktitel, Name des Rechtsinhabers) in einer Datenbank abgespeichert. Im zweiten Verfahrensabschnitt, während der *recognition phase*, wird die auf Identität mit einem Multimediawerk, dessen Fingerabdruck in der Datenbank gespeichert wurde, zu überprüfende Datei durch die Content-Identification-Technologie auf gleiche Weise analysiert wie im Rahmen der *training phase*, d.h. ein Fingerabdruck erstellt, der mit dem in der Datenbank abgespeicherten Fingerabdrücken abgeglichen wird. Ergibt dieser Abgleich einen hohen Grad an Übereinstimmung mit einem dieser Fingerabdrücke, meldet die Technologie diese Übereinstimmung unter Angabe des Grads der Übereinstimmung mit dem möglicherweise betroffenen Multimediawerk. Vgl. hierzu *Bechtold*, DRM, 2002, S. 92; *Herre*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 93, 94.

III. Qualitätsmerkmale und Treffsicherheit von Content-Identification-Technologien

Die Qualität einer Content-Identification-Technologie bemisst sich daran, ob sie in Bezug auf ihre Treffsicherheit bestimmte Anforderungen erfüllt. Sie muss zum einen robust sein, was bedeutet, dass die Technologie den Inhalt einer Datei auch dann identifizieren können muss, wenn an der Datei bestimmte Manipulationshandlungen vorgenommen wurden, wie beispielsweise eine Veränderung der Formatierung der Datei oder Änderung des in der Datei enthaltenen Inhalts selbst, beispielsweise der Tonhöhe oder der Geschwindigkeit der Ton- oder Bildfolge etc.[612] Auch muss eine Identifikation möglich sein, wenn nur Bruchstücke des Multimediawerks vorliegen. Weiterhin müssen *false positives* ausgeschlossen sein, d.h. es dürfen keine Übereinstimmungen angezeigt werden, obwohl der zu prüfende Inhalt mit keinem der in der Datenbank hinterlegten Fingerabdrücke von urheberrechtlich geschützten Multimediawerken übereinstimmt.

Ein weiteres Erfordernis ist die „signature compactness", d.h. ein möglichst geringes Datenvolumen des extrahierten Fingerabdrucks, da eine Content-Identification-Technologie regelmäßig große Mengen unterschiedlicher Multimediawerke zu erkennen in der Lage sein muss, wofür Voraussetzung ist, dass Fingerabdrücke all dieser Multimediawerke in der zugehörigen Datenbank hinterlegt werden. Dennoch muss das Datenvolumen der Datenbank technologisch beherrschbar bleiben. Dabei steht diese Notwendigkeit der Minimierung der Daten des Fingerabdrucks im Spannungsfeld mit der Anforderung, die Inhalte möglichst sicher zu identifizieren, was wiederum die Unterschreitung einer gewissen Mindestmenge an Referenzdaten in Bezug auf den gespeicherten Fingerabdruck verbietet.[613] Weiterhin ist eine gewisse Schnelligkeit in Bezug auf die Analyse der zu prüfenden Inhalte und den Vergleich mit den in der Datenbank eingespeisten Fingerabdrücken notwendige Voraussetzung für die Effizienz und damit für die praktischen Einsetzbarkeit der Content-Identification-Technologie.[614]

Generell ist die Treffsicherheit von Content-Identification-Technologien umstritten. Nach der Information Technology & Innovation Foundation sind Content-Identification-Technologien „mature, highly accurate and widely available".[615]

612 *Herre*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 93, 95. Manipulationen wie die Rotation des Bildwinkels, Verfälschungen von Einzelbildern oder die Abänderung des Farbabgleichs machen Content-Identification-Technologien vor allem im Zusammenhang mit der Identifikationen von Film- und Videowerken für Fehler anfällig, vgl. *Germain*, Dusting for Copyright Clues With Digital Fingerprinting Tech, TechNewsWorld, 22.08.2008, http://www.technewsworld.com/story/64249/.html.?wlc=1247835959 (zuletzt abgerufen am 01.07.2010).

613 *Herre*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 93, 95, 96.

614 *Herre* s.o.

615 *Castro/Bennett/Andes*, Steal these Policies, ITIF, 2009, S. III.

Auch nach Angaben des Internetdienstes iMesh liegt die Trefferquote der von diesem Dienst eingesetzten Content-Identification-Technologie des Anbieters Audible Magic bei 99 Prozent und sind insbesondere keine Probleme mit *false positives* bekannt.[616] Ebenso beansprucht YouTube für seine proprietär entwickelte Content-ID-Technologie[617] eine hohe Treffsicherheit. Allerdings wird gerade die Trefferquote dieser Content-Identification-Technologie oftmals in Zweifel gezogen.[618]

IV. Anbieter

Da die Verfahren für die Identifikation von Tonaufnahmen einerseits und von Filmwerken andererseits stark voneinander abweichen, ist in Bezug auf die Anbieter von Content-Identification-Technologien zu unterschieden, ob es sich um eine Technologie zur Erkennung von Audio- oder Videoinhalten handelt. Zwar ist es grundsätzlich möglich, ein Filmwerk auch auf der Grundlage einer reinen Audio-Filtertechnologie identifizieren zu lassen, allerdings sind die Anhaltspunkte zur Identifikation dann zwangsläufig auf die darin enthaltenen Audioelemente begrenzt. Naheliegend ist eine in dieser Weise beschränkte Identifikation für Musikvideos, da es den Rechtsinhabern hier grundsätzlich nur um die Durchsetzung ihrer Rechte in Bezug auf die darin verwendete Tonaufnahme geht, da solche Videos vornehmlich der Vermarktung der der Tonaufnahme dienen.[619] Für die Identifikation „reiner" Filmwerke wurden jedoch mittlerweile spezielle Technologien entwickelt.

Im Audiobereich gehört das Unternehmen Audible Magic Corp. („Audible Magic") zu den wichtigsten Anbietern. So bekannte Unternehmen wie die sozialen Netzwerke Facebook und MySpace, der Sender MTV sowie die Videoplattformen Veoh und YouTube gehören zu den Kunden, die innerhalb ihrer Dienste die Tech-

616 *Ohne Autor*, The End of Free Trade? How YouTube and MySpace will stop users from sharing copyrighted content, Newsweek Web Exclusive, 20.10.2006, http://www.newsweek.com/id/45365 (zuletzt abgerufen am 01.07.2010).

617 Vgl. 7. Kapitel, Teil B.I.4.c.

618 Vgl. beispielsweise *Steinert-Threlkeld*, YouTube's video ID system: is 75 percent good enough?, in: ZDNet Undercover: YouTube's Video Identification System, November 2008, S. 3.

619 Daher finden sich auf YouTube beispielsweise oftmals „stumme" Musikvideoclips, da die Rechtsinhaber nur den Audioteil ausfiltern lassen. Durch diese Vorgehensweise bezwecken die Rechtsinhaber, das technisch mögliche isolierte Ausschneiden des Audioteils aus einem gestreamten Videoclip zu verhindern. Der stumme Videoclip wird jedoch auf dem Internetdienst belassen, um dessen Marketingeffekt auszunutzen, d.h. Musikfans durch den Videoclip auf das Musikstück neugierig zu machen und dazu zu animieren, dass zugehörige Musikstück auf legalem Wege zu erwerben.

nologie dieses Anbieters einsetzen,[620] deren Ergebnisse angeblich zu 98 Prozent zutreffend sind.[621] Die von Audible Magic im Zusammenhang mit seiner Technologie geschaffene Datenbank enthält mittlerweile Informationen über mehr als sechs Millionen verschiedene Tonaufnahmen, Filmwerke und Softwareprogramme und wird auf der Grundlage neuer Informationen, die Audible Magic von den Rechtsinhabern zur Verfügung gestellt werden, ständig erweitert und aktualisiert.[622] Im Anschluss an die Identifizierung stellt die Content-Identification-Technologie von Audible Magic den Rechtsinhabern verschiedene Optionen zur Verfügung, wie mit einem Multimediawerk nach dessen Identifikation weiter zu verfahren ist (beispielsweise Nachverfolgung der Nutzung, Zuschaltung von Werbung, Hinzufügung von Erwerbsoptionen).

Für den Filmbereich galt die Entwicklung von Content-Identification-Technologien noch bis vor kurzem als höchst problematisch. Denn aufgrund der Komplexität von Filmdateien und der damit einhergehenden Bandbreite an Manipulationsmöglichkeiten bereitet die Erstellung von digitalen Fingerabdrücken von Filmwerken größere Schwierigkeiten als bei Tonaufnahmen.[623] Zudem werden weit mehr filmische Inhalte ständig neu veröffentlicht als Tonaufnahmen, weswegen es angesichts der ständig wachsende Menge an neuen Inhalten eine große Herausforderung darstellt, die zur effektiven Filterung erforderlichen Datenbanken zu aktualisieren.[624] Im Jahr 2007 zeichnete sich jedoch ab, dass auch die Rechtsinhaber im Filmbereich zunehmend auf Content-Identification-Technologien beim Schutz von Urheberrechten im Internet setzen, als Motion Picture Laboratories, Inc. („MovieLabs“) ein Projekt initiierte, in dessen Rahmen die Effizienz der zu dieser Zeit verfügbaren Content-Identification-Technologien getestet wurde.[625] Dabei wurde in einer ersten Versuchsreihe die Treffsicherheit der Technologien der teilnehmenden Anbieter bei der Identifikation von 1000 Videoclips unterschiedlichster Formate und Qualität geprüft. Unter den teilnehmenden Technologieanbietern

620 Vgl. die Auflistung der „Content Identification Services Customers“ des Unternehmens, http://audiblemagic.com/clients-partners/contentsvcs.asp (zuletzt abgerufen am 01.07.2010). Für eine ausführliche Beschreibung der Funktionsweise der von Audible Magic angebotenen Technologie vgl. *Wilkinson*, Musical Fingerprints, Electronic Musician, 01.09.2003, http://www.emusician.com/mag/tech/emusic_musical_fingerprints/index.html (zuletzt abgerufen am 01.07.2010).

621 *Wilkinson* s.o.

622 Vgl. die Beschreibung der „Content Identification Services“ des Unternehmens, http://audiblemagic.com/products%2Dservices/contentsvcs (zuletzt abgerufen am 01.07.2010).

623 *Rosenblatt*, 2006 Year in Review: DRM Technologies, DRM Watch, 21.12.2006, http://www.drmwatch.com/drmtech/article.php/3650401 (zuletzt abgerufen am 01.07.2010).

624 *Rosenblatt* s.o.

625 *Rosenblatt*, MovieLabs Shows Results of Fingerprint Testing, DRM Watch, 27.09.2007, http://www.drmwatch.com/watermarking/article.php/3702101 (zuletzt abgerufen am 01.07.2010).

schnitt das Unternehmen Vobile[626] am besten ab, gefolgt von den Technologien etablierter Anbieter wie Audible Magic und Gracenote. Nach dieser ersten Testreihe erklärte sich Harry Weinstein, der Präsident von MovieLabs, dass er Digital-Fingerprinting Technologien für den Schutz urheberrechtlich geschützter Filmwerke einsatzbereit halte.[627]

Das Unternehmen Auditude bietet eine Video-Fingerprinting-Technologie an, mit deren Hilfe Rechtsinhaber digitale Kopien von Filmwerken im Internet aufspüren[628] und die identifizierten Filmdateien mit Werbebotschaften und weiterführenden Informationen versehen können.[629] Im Rahmen einer Kooperation zwischen Auditude, dem Sozialen Netzwerk MySpace und dem Unternehmen MTV Networks wird diese Technologie dazu eingesetzt, die auf MySpace eingestellten Inhalte auf urheberrechtlich geschützte Inhalte von MTV Networks zu durchsuchen.[630] Zu diesem Zweck werden die von den Nutzern auf den Web 2.0-Dienst hochgeladenen Videoclips mit einer von Auditude erstellten Datenbank abgeglichen, die Informationen über ca. 250 Millionen Filmwerke enthält.[631] Ergibt dieser Abgleich eine Übereinstimmung, wird die betroffene Filmdatei mit einem Hinweis auf die Originalquelle, einem Verweis auf eine Kaufmöglichkeit und/oder einer Werbebotschaft versehen.[632] Die daraus gewonnen Einnahmen teilen sich MTV und MySpace.[633]

Ein Beispiel für einen deutschen Anbieter einer Video-Fingerprinting-Technologie ist die iPharro Media GmbH mit Sitz in Darmstadt, ein im Jahr 2006 gegründeter Ableger des Fraunhofer Instituts für Graphische Datenverarbeitung.[634] iPharros bisher erfolgreichstes Produkt ist die „MediaSeeker"-Software, die es ihren

626 *Stone*, One Anti-Piracy System to Rule Them All, New York Times, Bits Weblog, 21.9.2007, http://bits.blogs.nytimes.com/2007/09/21/one-anti-piracy-system-to-rule-them-all/(zuletzt abgerufen am 01.07.2010).

627 *Stone* s.o.

628 *Sandoval*, Feature films coming to YouTube, CNET News, 06.11.2008, http://news.cnet.com/8301-1023_3-10083481-93.html?part=rss&tag=feed&subj=News-DigitalMedia (zuletzt abgerufen am 01.07.2010).

629 *Rosenblatt*, Auditude's Fingerprinting Powers Contextual Ad Service on MySpace, DRM Watch, 06.11.2008, www.drmwatch.com/watermarking/article.php/3783336 (zuletzt abgerufen am 01.07.2010).

630 *Heise Online*, MySpace und MTV testen neues Vermarktungsmodell für Online-Videos, heise online, 03.11.2008, http://www.heise.de/newsticker/meldung/118328 (zuletzt abgerufen am 01.07.2010); *Chartier*, MySpace inks advertising deal with MTV networks, Ars Technica, 03.11.2008, http://arstechnica.com/news.ars/post/20081103-myspace-inks-advertising-deal-with-mtv-networks.html (zuletzt abgerufen am 01.07.2010).

631 *Heise Online*, MySpace und MTV testen neues Vermarktungsmodell für Online-Videos, heise online, 03.11.2008, http://www.heise.de/newsticker/meldung/118328 (zuletzt abgerufen am 01.07.2010).

632 *Heise Online* s.o.

633 *Heise Online* s.o.; *Rosenblatt*, Auditude's Fingerprinting Powers Contextual Ad Service on MySpace, DRM Watch, 06.11.2008, www.drmwatch.com/watermarking/article.php/3783336 (zuletzt abgerufen am 01.07.2010).

634 http://www.igd.fraunhofer.de.

Nutzern erlaubt, mehrere Fernsehkanäle mithilfe einer Video-Fingerprinting-Technologie auf rechtlich geschützte Inhalte hin zu überwachen. Zu den Kunden des Unternehmens zählt unter anderem das Unternehmen Nielsen Media Research, die eine iPharro-Technologie zur weltweiten Überwachung und Nachverfolgung von Werbebotschaften im Rahmen der werbestatistischen Datensammlung einsetzt, sowie das Zweite Deutsche Fernsehen (ZDF). Im Juni 2009 kündigte iPharro ein neues Produkt an, den „iPharro Enterprise Server", mit dessen Hilfe es nach Angaben des Unternehmens möglich sein soll, die Funktionen der Video-Fingerprinting-Technologie zur Indexierung und Identifizierung von Filmwerken effizient und umfassend in den Betriebsablauf von medienabhängigen Unternehmens zu integrieren.[635]

V. Die „ContentID"-Technologie der Videoplattform YouTube

Im Oktober 2007 verkündete Google auf seiner Webseite[636] die Implementierung einer Technologie auf seiner Videoplattform YouTube, mit deren Hilfe Videoclips mit urheberrechtlich geschützten Inhalten identifiziert und daraufhin je nach Wunsch des jeweils betroffenen Rechtsinhabers entweder entfernt oder aber durch die Hinzufügung von Werbebotschaften kommerzialisiert werden können sollen.[637] Diese sogenannte „ContentID-Technologie"[638] besteht aus zwei Komponenten: einer Audio-Fingerprinting-Technologie des Anbieters Audible Magic,[639] sowie einer Video-Fingerprinting-Technologie, die von Googles Ingenieuren intern entwickelt wurde (nachfolgend „Video-ID" genannt). Anfang 2007 hatte YouTube mit dem Einsatz der Audio-Fingerprinting-Technologie von Audible Magic im Zusammenhang mit seiner Kooperation mit einigen Musikunternehmen

635 Vgl. die Ankündigung des Unternehmens anlässlich der DAM (Digital Asset Management) 2009, abrufbar unter http://www.ipharro.com/all_Images/PDFs/english/iPharro_DAM_ES_1_6_09.pdf (zuletzt abgerufen am 01.07.2010.).

636 *King*, Latest Content ID Tool for YouTube, The Official Google Weblog, 15.10.2010 http://googleblog.blogspot.com/2007/10/latest-content-id-tool-for-youtube.html (zuletzt abgerufen am 01.07.2010).

637 *Heise Online*, YouTube startet automatische Video-Identifizierung, 16.10.2007, http://www.heise.de/newsticker/meldung/97434 (zuletzt abgerufen am 01.07.2010); *Hendrickson*, YouTube Tries a Little Harder to Protect Copyright Holders, TechCrunch, 15.10.2007, http://www.techcrunch.com/2007/10/15/youtube-tries-a-little-harder-to-protect-copyright-holders (zuletzt abgerufen am 01.07.2010.).

638 Vgl. die Beschreibung der ContentID-Technologie auf YouTube, http://www.youtube.com/t/contentid (zuletzt abgerufen am 01.07.2010); vgl. auch die frühere Ankündigung der Beta-Version, YouTube-Videoidentifizierung - Beta-Version, http://www.youtube.com/t/video_id_about (zuletzt abgerufen am 01.07.2010).

639 Vgl. vorhergehendes Kapitel.

begonnen, darunter Warner Music, Sony und Universal.[640] Die Technologie überprüft, sobald ein Nutzer einen Videoclip auf die Plattform hochzuladen versucht, ob der Audio-Teil des Videoclips mit dem digitalen Fingerabdruck einer der in der Datenbank von Audible Magic gespeicherten Tonaufnahmen übereinstimmt.

YouTubes Entscheidung, zur Identifizierung urheberrechtlich geschützter Inhalte in Videoclips anders als bei der Identifizierung von reinen Audioelementen nicht auf einen externen Anbieter zurückzugreifen, sondern eine eigene Technologie zu entwickeln geht angeblich darauf zurück, dass ein Testlauf ergeben hätte, dass die in Betracht kommenden bereits existierenden Technologien YouTubes Anforderungen nicht entsprechen würde.[641] Die daraufhin intern entwickelte Video-ID-Technologie basiert auf der Prämisse, dass jedes Filmwerk bestimmte charakteristische, einzigartige Eigenschaften besitzt, die es ermöglichen, dieses Werk oder Teile davon mit Hilfe eines Algorithmus, der diese Eigenschaften verkörpert, auch in kurzen Videoclips wieder zu erkennen. Über die Details der Technologie hält sich YouTube jedoch sehr bedeckt. So beschränken sich die Pressemitteilungen insoweit auf die eher vage Aussage, dass „key visual aspects" verwendet würden, um die hochgeladenen Videoclips mit Referenzmaterial von urheberrechtlich geschützten Werken, welches die Rechtsinhaber YouTube zunächst zur Verfügung stellen müssen, wenn sie ihre Werke durch die Video-ID-Technologie schützen lassen wollen, abzugleichen.[642] Auf der Grundlage dieses Referenzmaterials erstellt YouTube einen digitalen Fingerabdruck, der in eine Datenbank eingespeist wird.[643] Findet die ContentID-Technologie geschütztes Material auf, so wird dieses je nach Wunsch des betroffenen Rechtsinhabers entweder von der Plattform gelöscht, seine Nutzung zur Erstellung statistischer Daten überwacht (Anzahl der Abrufe etc.) oder aber Werbung zugeschaltet, deren Erlös zwischen YouTube und dem Rechtsinhaber geteilt wird. Nach Angaben von YouTube entscheidet sich mittlerweile die überwiegende Mehrheit der Rechtsinhaber, ihre Inhalte auf der Webseite zu belassen, d.h. ihre Nutzung an YouTube zu lizenzieren und von den

640 *Delaney*, YouTube to Test Software To Ease Licensing Fights, The Wall Street Journal, 12.06.2007, http://online.wsj.com/article/SB118161295626932114.html (zuletzt abgerufen am 01.07.2010); *Li/Auchard*, YouTube to test video ID with Time Warner, Disney, Reuters, 12.06.2007, http://www.reuters.com/article/wtMostRead/idUSWEN871820070612 (zuletzt abgerufen am 01.07.2010).

641 *Delaney* s.o.

642 *Chen*, The state of our video ID tools, The Official Google Weblog, 14.06.2007, http://googleWeblog.Weblogspot.com/2007/06/state-of-our-video-id-tools.html (zuletzt abgerufen am 01.07.2010).

643 *Associated Press*, For YouTube, a System to Halt Copyright-Infringement Videos, The New York Times, 28.07.2007, http://www.nytimes.com/2007/07/28/business/28google.html (zuletzt abgerufen am 01.07.2010).

im Zusammenhang mit den Inhalten erzielten Werbeeinnahmen zu profitieren.[644] Weiterhin ist Google nach eigenen Angaben dabei, eine Technologie zu entwickeln, die es Rechtsinhabern ermöglicht, Werbebotschaften unmittelbar in die von Nutzern hochgeladenen Inhalte einzubetten.[645]

Umstritten ist, wie treffsicher die ContentID-Technologie tatsächlich ist; YouTube selbst äußert sich dazu nicht, ebensowenig wie zu der Höhe der Umsätze, die es durch die Zuschaltung von Werbung zu den Videoclips erzielt. So war beispielsweise ein Videoclip mit einem in den USA sehr populären Sketch der „Saturday Night Live"-Show betreffend die Gouverneurin Sarah Palin noch tagelang nach seiner Erstausstrahlung über den Fernsehsender NBC auf YouTube abrufbar, obwohl NBC Universal zu denjenigen Medienunternehmen gehört, die ihre geschützten Inhalte von der Videoplattform entfernen lassen, um interessierte Nutzer auf ihre eigenen Webseiten bzw. die in Gemeinschaft mit anderen Medienunternehmen betriebene, konkurrierende Videoplattform Hulu umzusteuern.[646] Es ist somit davon auszugehen, dass die Technologie derzeit jedenfalls noch nicht völlig fehlerfrei arbeitet.[647]

C. Einsatzmöglichkeiten für Content-Identification-Technologien im Web 2.0

Content-Identification-Technologien können entweder rein repressiv zur Beseitigung von Multimediawerken eingesetzt werden, die auf einem Web 2.0-Dienst unerlaubt der Öffentlichkeit zugänglich gemacht werden. Darüber hinaus ermöglichen sie jedoch auch die Kommerzialisierung von Multimediawerken in Web 2.0-Diensten im Zusammenhang mit sogenannten *ad-supported business models*.

644 *King*, Making money on YouTube with Content ID, The Official Google Weblog 27.08.2009, http://googleblog.blogspot.com/2008/08/making-money-on-youtube-with-content-id.html (zuletzt abgerufen am 01.07.2010).

645 *Sandoval*, Could peace be near for YouTube and Hollywood?, CNET News, 23.07.2008, http://news.cnet.com/8301-1023_3-9996905-93.html (zuletzt abgerufen am 01.07.2010).

646 *Steinert-Threlkeld*, YouTube's video ID system: is 75 percent good enough?, in: ZDNet Undercover: YouTube's Video Identification System, November 2008, S. 3.

647 *Steinert-Threlkeld*, s.o. Google selbst die Entwicklung der Technologie einmal als *„one of the most technologically complicated tasks that we have ever undertaken"* bezeichnet, vgl. The state of our video ID tools, The Official Google Weblog, 14.06.2007, abrufbar unter http://googleblog.blogspot.com/2007/06/state-of-our-video-id-tools.html (zuletzt abgerufen am 01.07.2010) .

Ursprünglich bestand der hauptsächliche Zweck des Einsatzes von Content-Identification-Technologien im Rahmen von Internetdiensten darin, hierdurch das unerlaubte Hochladen von digitalen, urheberrechtlich geschützten Multimediawerken auf bestimmten Plattformen von vornherein zu verhindern bzw. solche Dateien nach ihrem Hochladen auf einer Webseite zu identifizieren und wieder zu entfernen.[648]

Diesen Ansatz verfolgt nach wie vor beispielsweise der US-amerikanische Medienkonzern NBC Universal. Rick Cotton, Executive Vice President und General Counsel des Unternehmens, ist einer der prominentesten Vertreter der Auffassung, dass der Einsatz von Content-Identification-Technologien beim Aufbau profitabler Vertriebswege im Zusammenhang mit dem Internet in Zukunft eine wichtige Rolle spielen wird, und eine darauf gerichtete Zusammenarbeit zwischen den Betreibern von Web 2.0-Diensten einerseits und den Rechtsinhabern andererseits unabdingbar ist.[649] Dementsprechend werden auf Videoplattformen wie YouTube, Dailymotion und Veoh Content-Identification-Technologien zur Entfernung urheberrechtlich geschützten Materials des Unternehmens eingesetzt, in Kombination mit dem gezielten Aufbau von durch den Konzern gesteuerten Internetangeboten zum Konsum der unternehmenseigenen TV-Serien und –Shows. Nach Angaben von Cotton ist es dem Unternehmen auf diese Weise gelungen, dass das Filmmaterial zu den Olympischen Spielen 2008 im Internet zu 99 Prozent über die Webseiten NBC.com oder NBCOlympic.com angesehen wurde.[650] Denn indem Kopien von jeder Ausstrahlung der Olympischen Spiele umgehend an die Plattformbetreiber sowie die Technologieanbieter Audible Magic und Vobile gesendet wurden, auf deren Grundlage die erforderlichen digitalen Fingerabdrücke generiert werden konnten,

648 *Herre*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003, S. 93, 98.

649 *Sandoval*, NBC finds formula for fighting pricay, CNET News, 23.09.2008, http://news.cnet.com/8301-1023_3-10048949-93.html?part=rss&tag=feed&subj=News-DigitalMedia (zuletzt abgerufen am 01.07.2010); *Chevalier*, Commerce in the era of ‚free' – a common challenge for creative industries, in: *IFPI*, Digital Music Report 2009, S. 4.

650 *Rick Cotton*, zitiert bei *Chevalier*, Commerce in the era of ‚free' – a common challenge for creative industries, in: *IFPI*, Digital Music Report 2009, S. 4: *„This was the most viewed TV production in American history, and the overwhelming access point for online viewers was at nbcolympics.com – and the thing that essentially eliminated pirated olympic content from video sharing sites was content recognition technology and filtering"*; vgl. auch *Steinert-Threlkeld*, YouTube's video ID system: is 75 percent good enough?, in: ZDNet Undercover: YouTube's Video Identification System, November 2008, S. 12. Ähnlich erfolgreich war das Unternehmen angeblich im Falle einer Parodie der Vizepräsidentschaftskandidatin Sarah Palin, da sämtliche illegale Mitschnitte dieser im Rahmen einer Saturday-Night-Live-Show ausgestrahlten Parodie auf YouTube identifiziert und entfernt werden konnten, vgl. *Sandoval*, NBC finds formula for fighting pricay, CNET News, 23.09.2008, http://news.cnet.com/8301-1023_3-10048949-93.html?part=rss&tag=feed&subj=News-DigitalMedia (zuletzt abgerufen am 01.07.2010).

konnten unautorisiert auf den einschlägigen Videoplattformen eingestellte Mitschnitte der Spiele innerhalb kürzester Zeit durch die jeweils eingesetzten Content-Identification-Technologien identifiziert und blockiert oder nachträglich entfernt werden.[651] Ergänzend seien den Nutzern auf NBCs eigenen Webseiten sowie auf der Internetplattform Hulu, die NBC Universal gemeinsam mit dem Unternehmen News Corp. betreibt, attraktive Alternativen zum Abruf der Aufzeichnungen der Spiele geboten worden. Die Nutzer hätten schnell realisiert, dass auf YouTube nur Standbilder der Spiele verfügbar waren, und seien dann auf die Seiten von NBCOlympics.com gewechselt.[652]

Damit ist NBC Universal ein Beispiel für ein Unternehmen, das in dem Einsatz von Content-Identification-Technologien auf Web 2.0-Diensten zwar eine wesentliche Voraussetzung für den Erfolg ihrer neuen Geschäftsstrategie im Internet sieht, diese Technologien jedoch in erster Linie zu repressiven Zwecken einsetzt. Dieser Ansatz ist Teil der Strategie, die Nutzerströme umzusteuern und hierdurch eigene, von den klassischen Web 2.0-Diensten unabhängige Plattformen zur Präsentation und Vermarktung von Multimediawerken zu schaffen. Auf diese Weise sollen die Nutzer nach und nach daran gewöhnt werden, auf von der Multimediaindustrie angebotene, legale Dienste zum Konsum von Multimediawerken über das Internet zurückzugreifen.

II. Kommerzialisierung von Multimediawerken in Web 2.0-Diensten

Allerdings können Content-Identification-Technologien nicht nur zur Entfernung von urheberrechtswidrigem Material aus Web 2.0-Diensten genutzt werden, sondern besteht ein weiteres erhebliches Potenzial dieser Technologien darin, urheberrechtlich geschütztes Material dort, wo es von Nutzern eingestellt wird, vor allem im Zusammenhang mit werbefinanzierten Geschäftsmodellen[653] zu kommerzialisieren.

Ein konkretes Beispiel für diese neue Möglichkeit ist das Videoportal YouTube. Mit der zuvor dargestellten ContentID-Technologie[654] trägt dieser Internetdienst zunehmend dazu bei, dass die Rechtsinhaber mit den auf der Plattform eingestellten Filmwerken, an dem sie Rechte halten, unmittelbar Geld verdienen, indem die Inhalte mit Werbebotschaften verbunden werden und die daraus erzielten Einnahmen

651 *Steinert-Threlkeld*, YouTube's video ID system: is 75 percent good enough?, in: ZDNet Undercover: YouTube's Video Identification System, November 2008, S. 12.
652 *Sandoval*, NBC finds formula for fighting pricay, CNET News, 23.9.2008, http://news.cnet.com/8301-1023_3-10048949-93.html?part=rss&tag=feed&subj=News-Digital-Media (zuletzt abgerufen am 01.07.2010).
653 Vgl. 7. Kapitel, Teil A.III.2.d.
654 Vgl. 7. Kapitel, B.I.4.c.

anteilig an die Rechtsinhaber ausgezahlt werden. Zu diesem Zweck hat YouTube beispielsweise mit allen großen Tonträgerunternehmen Verträge geschlossen, wonach deren geschützte Tonaufnahmen und die zugehörigen Musikvideos auf der Plattform öffentlich zugänglich gemacht werden dürfen und YouTube im Gegenzug einen Teil der in diesem Zusammenhang erzielten Werbeeinnahmen an die Unternehmen auszahlt.[655] Zwar sind Details dieser Vereinbarungen nicht bekannt, allerdings wird vermutet, dass die durch die Zuschaltung von Werbung erzielten Einnahmen ursprünglich hälftig zwischen dem jeweiligen Rechtsinhaber und YouTube geteilt wurden. Dieser Anteil war den Tonträgerunternehmen jedoch bald zu gering, weswegen Warner Music Group sich beim Auslaufen seiner Vereinbarung mit YouTube im Dezember 2008 zunächst weigerte, die Kooperation zu gleichen Bedingungen fortzuführen; dies hatte zur Folge, dass alle Inhalte des Unternehmens wieder aus dem Internetdienst entfernt werden mussten.[656] Im September 2009 kam es dann aber doch noch zu einer Einigung, wonach Warner Music Group nunmehr einen höheren Anteil der erzielten Einnahmen erhält und zudem berechtigt ist, die im Zusammenhang mit den Videoclips des Unternehmens verfügbaren Werbeplätze selbständig zu verkaufen bzw. durch Dritte verkaufen zu lassen.[657]

Nach Angaben von YouTube werden urheberrechtlich geschützte Videoclips nach ihrer Identifizierung durch die ContentID-Technologie zum weit überwiegenden Teil auf Wunsch des Rechtsinhabers nicht von dem Internetdienst entfernt, sondern mit einer Werbebotschaft oder mit Informationen über das jeweilige Werk verbunden und auf der Plattform belassen.[658] Damit werden Content-Identificati-

655 *Heise Online*, Warner Music und YouTube: Ende der Eiszeit?, 11.07.2009, http://www.heise.de/newsticker/meldung141870 (zuletzt abgerufen am 01.07.2010); *Sandoval*, Warner Music Group and YouTube talking again, 10.07.2009, http://news.cnet.com/8301-1023_3-10284399-93.html?part=rss&tag=feed&subj=News-DigitalMedia (zuletzt abgerufen am 01.07.2010).

656 *Ohne Autor*, YouTube darf wieder Warner-Videos zeigen, tagesschau.de, 30.09.2009, http://www.tagesschau.de/warnertube100.html (zuletzt abgerufen am 01.07.2010); *Heise Online*, Bericht: YouTube und Warner einigen sich über Musikvideo-Lizenzen, heise online, 29.09.2009, http://www.heise.de/newsticker/meldung/Bericht-YouTube-und-Warner-einigen-sich-ueber-Musikvideo-Lizenzen-798101.html (zuletzt abgerufen am 01.07.2010).

657 *Heise Online* s.o.

658 *Sandoval*, Could peace be near for YouTube and Hollywood?, CNET News, 23.07.2008, http://news.cnet.com/8301-1023_3-9996905-93.html (zuletzt abgerufen am 01.07.2010). Diese Möglichkeit zur Kommerzialisierung von Videclips steht nunmehr außer den großen Major-Labels, Hollywoodstudios und anderen sog. „premium partners" auch ganz normalen Nutzern zur Verfügung. Abhängig von der Anzahl der Abrufe eines Videoclips (sog. Viralität) sowie unter der Voraussetzung der Einhaltung der Nutzungsbedingungen von YouTube entscheidet der Internetdienst darüber, ob ein Video das Potential für Profitabilität aufweist - wenn ja, erhält der Nutzer eine Email und kann sich entscheiden, seinen Videoclip zur Verschaltung mit Werbung freizugeben, in welchem Fall er dann einen Teil der Einnahmen erhält; vgl. Shenaz Zack, In the future, everyone will monetize their 15 minutes, 25.08.2009, http://googleblog.blogspot.com/2009/08/in-future-everyone-will-monetize-their.html (zuletzt abgerufen am 01.07.2010).

on-Technologien jedoch zum Bindeglied zwischen den Gefahren und den Chancen des Web 2.0. Denn durch sie wird es möglich, ein von einem Nutzer ohne Erlaubnis des Rechtsinhabers auf einen Web 2.0-Dienst hochgeladenes Multimediawerk in einen Kontext einzubetten, der die Kommerzialisierung des Werks zum Vorteil des Rechtsinhabers im Rahmen eines werbefinanzierten Geschäftsmodells ermöglicht. Dies bedeutet, dass nach diesem Ansatz ein Rechtsinhaber umso mehr von seinem Werk profitiert, je öfter es auf einem Web 2.0-Dienst eingestellt wird, da ihm hieraus jedes Mal ein Anspruch auf Werbeeinnahmen gegen den Betreiber des Internetdienstes erwächst. Vor diesem Hintergrund könnten sich die „Gefahren" der Digitalisierung jedoch als ein großer Vorteil für die Rechtsinhaber entpuppen. Denn dann könnten die mannigfachen Möglichkeiten der Vervielfältigung und Verbreitung von digitalen Multimediawerken durch die Nutzer im Rahmen von werbefinanzierten, mit Content-Identification-Technologien ausgestatteten Web 2.0-Diensten zu dem Ergebnis führen, dass die Rechtsinhaber hiervon in ebenso vielfältiger Weise aufgrund der Kommerzialisierung ihrer Werke durch die zugeschalteten Werbebotschaften profitieren können. Im Ergebnis hinge dann der wirtschaftliche Erfolg eines Multimediawerks von dessen – sich im Umfang der Verbreitung innerhalb von Web 2.0-Diensten niederschlagenden – Popularität bei den Nutzern ab, ein Ergebnis, dass sowohl demokratischen als auch marktwirtschaftlichen Grundsätzen entspricht.

8. Kapitel: Auswirkungen von Content-Identification-Technologien auf die Haftung von Betreibern von Web 2.0-Diensten für Urheberrechtsverletzungen der Nutzer

Auch angesichts der Verfügbarkeit und des zunehmend verbreiteten Einsatzes von Content-Identification-Technologien fordern die Rechtsinhaber derzeit verstärkt, ISPs in Bezug auf die Aufdeckung und Beseitigung von Urheberrechtsverletzungen (sogenanntes „copyright policing") innerhalb ihrer Internetdienste mehr in die Pflicht zu nehmen. Fraglich ist jedoch die rechtliche Begründbarkeit einer solchen Verpflichtung der ISPs nach der derzeitigen Rechtslage im US-amerikanischen Urheberrecht, insbesondere unter Berücksichtigung der Haftungsbeschränkung für Host-Provider gemäß 17 U.S.C. § 512(c). Diese Frage zu beantworten ist Gegenstand dieses Kapitels. Des Weiteren werden die in Bezug auf die US-amerikanische Rechtslage gefundenen Ergebnisse der gegenwärtigen deutsch-europäischen Situation gegenübergestellt und verglichen.

A. *Forderung der Rechtsinhaber nach einer stärkeren Beteiligung der Betreiber von Web 2.0-Diensten an der Durchsetzung von Urheberrechten*

Die Bemühungen der Multimediaindustrie richten sich gegenwärtig darauf, die Lasten des *copyright policing*, d.h. den zeitlichen, personellen und finanziellen Aufwand im Zusammenhang mit der Durchsetzung von Urheberrechten an Multimediawerken im Internet, ihrem Schwerpunkt nach auf die ISPs zu verlagern.[659] Dies ist der Hintergrund sowohl für das Bestreben, Access-Provider auf das bereits dargestellte Konzept der „Graduated Response" oder „Three Strikes Policy" zu verpflichten,[660] als auch für die nachfolgend dargestellte Forderung, Betreiber von Web 2.0-Diensten verstärkt zum Einsatz von Content-Identification-Technologien zum Auffinden und zur Beseitigung von urheberrechtswidrigem Material in ihren Internetdiensten zu verpflichten.

Angesichts der riesigen Datenmengen, die im Zeitalter des Web 2.0 tagtäglich neu auf Internetdienste hochgeladenen werden, hat sich die Auffindung von urheberrechtswidrigem Material zu einer sehr zeitaufwendigen und kostspieligen Aufgabe entwickelt.[661] Allein auf YouTube werden pro Minute etwa zehn Stunden neues Videomaterial eingestellt, was einer Menge von ca. 250.000 pro Tag neu auf die Videoplattform hochgeladenen Videoclips entspricht.[662] Dementsprechend sind beispielsweise beim Medienunternehmen Viacom ständig ein bis zwei Dutzend Angestellte allein damit beschäftigt, die auf die Videoplattform hochgeladenen Videoclips auf urheberrechtswidriges Material hin zu durchsuchen.[663] Jedoch kann auch ein ausschließlich auf diese Aufgabe konzentrierter Angestellter höchstens 40-50 Videos pro Stunde sichten, woraus hervorgeht, dass trotz eines solchen personellen Aufwandes nur ein Bruchteil des in Web 2.0-Diensten vorhandenen Materials tatsächlich überprüft werden kann.

Vor diesem Hintergrund halten es die Rechtsinhaber zunehmend für eine unbillige Belastung ihrerseits, diese gigantischen Datenmengen nach Urheberrechtsverletzungen durchsuchen und im Anschluss daran den Betreiber des Internetdienstes, innerhalb dessen das jeweilige urheberrechtswidrige Material aufgefunden wurde, hierauf aufmerksam machen zu müssen, wie dies beispielsweise das Verfahren zur Beseitigung von urheberrechtswidrigem Material gemäß 17 U.S.C.

659 *Seidenberg*, ABA Journal, February 2009, S. 47.
660 Vgl. 3. Kapitel, Teil B.II.3.a.
661 *Seidenberg*, ABA Journal, February 2009, S. 48.
662 *Seidenberg*, ABA Journal, February 2009, S. 49.
663 *Steinert-Threlkeld*, YouTube's video ID system: is 75 percent good enough?, in: ZDNet Undercover: YouTube's Video Identification System, November 2008, S. 3.

§ 512(c) vorsieht.[664] Auch kann bei einem solchen Prozedere der jeweilige Rechtsinhaber erst dann gegen Urheberrechtsverletzungen vorgehen, wenn das urheberrechtswidrige Material bereits auf einen Internetdienst hochgeladen wurde und die Rechtsverletzung damit bereits eingetreten ist. Dies bedeutet, dass die Rechtsinhaber erst eine Verletzung ihrer Rechte abwarten müssen, da sie erst nach der erfolgten Rechtsverletzung re-aktiv gegen diese vorgehen können. Hingegen könnte durch den Einsatz von Content-Identification-Technologien die Begehung von Urheberrechtsverletzungen noch vor deren Eintritt proaktiv verhindert werden, indem diese Technologien geschütztes Material bereits während des Hochladens erkennen und noch vor deren vollendeter Einstellung auf dem Web 2.0-Dienst ausfiltern könnten.[665] Nach der Argumentation der Rechtsinhaber führt der Einsatz von Content-Identification-Technologien durch Web 2.0-Dienste somit zu einer wesentlichen Vereinfachung und Beschleunigung des *copyright policing* und zudem zu einer Einsparung des Aufwandes an Zeit und Kosten, der derzeit insbesondere im Zusammenhang mit dem Einsatz von Mitarbeitern entsteht, die ausschließlich mit der Auffindung und Einleitung entsprechender Maßnahmen gegen Urheberrechtsverletzungen befasst sind.

I. Verpflichtung von Web 2.0-Diensten zum Einsatz von Content-Identification-Technologien auf Grundlage der „User Generated Content Principles"

Der Idealfall für die Rechtsinhaber wäre eine universell einsetzbare Content-Identification-Technologie, die flächendeckend von allen ISPs in ihren Internetdiensten eingesetzt werden müsste.[666] Dann würde die Last des *copyright policing* den ISPs obliegen, wohingegen die Rechtsinhaber sich darauf beschränken könnten, ausschließlich dem Anbieter dieser Technologie die Informationen zu überlassen, mit

664 Vgl. 8. Kapitel, Teil B.III.4.f; *Meyers*, 26 Cardozo Arts & Entertainment L. J. 935, 941(2009): "*Though on its face, DMCA section 512 appears to be a well-intentioned effort by Congress to balance the interests of copyright owners, user-generated content creators, and OSPs, many critics, including influential media and entertainment corporations, argue that the Act's fatal flaw lies in its emphasis on the copyright owner having to police his content for infringement.*"; *Beaty*, 13 Marq. Intell. Prop. L. Rev. 207, 224 (2009): *"The sheer volume of work that a copyright owner must put into monitoring websites on the Internet and filling out detailed reports to send to the websites puts a heavy burden on the copyright owner. The legislative intent behind the DMCA was not to put the entire burden on the copyright owner, but was to strike a balance between the rights of a copyright owner and the importance of allowing technology to expand without a constant fear of lawsuits.".*

665 *Rosenblatt* s.o.

666 *Bangemann*, Viacom's true desire: one copyright filter to rule them all, Ars Technica, 22.10.2007, http://arstechnica.com/news.ars/post/20071022-viacoms-true-desire-one-copyright-filter-to-rule-them-all.html?rel (zuletzt abgerufen am 01.07.2010).

Hilfe derer die zur Identifizierung notwendigen digitalen Fingerabdrücke ihrer urheberrechtlich geschützten Multimediawerke generiert werden können.[667]

Um dieses Ziel zu erreichen, haben die Rechtsinhaber eine branchenübergreifende Initiative initiiert, die darauf gerichtet ist, Anbieter von Web 2.0-Diensten zum Einsatz einer solchen Content-Identification-Technologien zu verpflichten. Im Oktober 2007 veröffentlichten mehrere führende Technologie- und Medienunternehmen, darunter Microsoft Corporation, CBS Corporation, The Walt Disney Company, Fox Entertainment Group, NBC Universal, Viacom, Veoh, Dailymotion und MySpace, gemeinsam entworfene Richtlinien, die sogenannten „Principles for User Generated Content Services" (nachfolgend „UGCP" oder „UGCP-Inititave").[668] In dieser unverbindlichen Absichtserklärung werden Regeln für den Umgang mit urheberrechtlich geschützten Inhalten formuliert für Internetdienste, die im Bereich des Web 2.0 tätig sind und nutzergenerierte Inhalte anbieten.[669] Die UGCP-Initiative verfolgt vor allem das Ziel, rechtswidrige Inhalte aus Web 2.0-Diensten zu eliminieren und die Rechte der Rechtsinhaber an urheberrechtlich geschützten Multimediawerken zu schützen. Dementsprechend ist ihre zentrale Forderung der standardmäßige Einsatz von Content-Identification-Technologien auf Web 2.0-Diensten zur Identifizierung von urheberrechtlich geschützten Multimediawerken, die von den Nutzern rechtswidrig auf einen Web 2.0-Dienst hochgeladen werden.[670] Im Anschluss an die Identifizierung sollen die Rechtsinhaber frei darüber entscheiden können, wie der ISP mit dem identifizierten Material zu verfahren hat, d.h. ob der Inhalt aus dem Web 2.0-Dienst entfernt werden muss oder aber auf der Webseite verbleiben kann, beispielsweise unter der Auflage der Zuschaltung von Werbebotschaften. Der Einsatz von Content-Identification-Technologien soll weiterhin unabhängig davon erfolgen, ob mit dem jeweiligen Rechtsinhaber, dessen Material mit Hilfe einer solchen Technologie identifiziert wird, eine Lizenzvereinbarung oder anderweitige Geschäftsverbindung in Bezug auf die Nutzung seines urheberrechtlich geschützten Materials im Rahmen des jeweiligen Internetdienstes besteht.[671]

667 *Rosenblatt*, Thoughts on Notice, Takedown, Fingerprints, and Filtering, DRM Watch, 15.03.2007, http://www.drmwatch.com/legal/article.php/3665921 (zuletzt abgerufen am 01.07.2010).

668 Die gemeinsame Presseerklärung sowie der Text der UGCP sind abrufbar unter http://www.ugcprinciples.com.

669 *Marr/Delaney*, Disney, Microsoft Lead Copyright Pact, WSJ.com, 19.10.2007, http://online.wsj.com/public/article_print/SB119269788721663302.html (zuletzt abgerufen am 01.07.2010).

670 Vgl. Ziff. 3 S. 1 UGCP: *"UGC Services should use effective content identification technology ("Identification Technology") with the goal of eliminating from their services all infringing user-uploaded audio and video content for which Copyright Owners have provided Reference Material (as described below)."*.

671 Vgl. Ziff. 3 e UGCP.

Im Gegenzug für die Verpflichtung der Betreiber von Web 2.0-Diensten zum Einsatz von Content-Identification-Technologien verpflichten sich die an der UGCP-Initiative teilnehmenden Rechtsinhaber, den Anspruch der ISPs auf eine unter dem *Copyright Act* gewährte Haftungsbeschränkung, wie beispielsweise der Safe-Harbor-Regelung für Host-Provider gemäß § 512(c), nicht anzugreifen. Darüber hinaus versprechen sie, generell von Klagen gegen ISPs in Bezug auf urheberrechtswidriges Material abzusehen, das trotz der UGCP-konformen Bemühungen des ISPs auf dessen Internetdienst verbleibt.[672] Der Anreiz für die Betreiber von Web 2.0-Diensten, sich der Initiative anzuschließen und auf ihren Internetdiensten Content-Identification-Technologien einzusetzen, besteht somit darin, hierdurch das Risiko erheblich minimieren zu können, von den Rechtsinhabern wegen Urheberrechtsverletzungen verklagt zu werden. [673]

In den einschlägigen Weblogs und News-Diensten wurden die UGCP vielfach wegen einer einseitigen Gewichtung zugunsten der Interessen der großen Hollywoodstudios und TV-Produktionsfirmen kritisiert. Denn durch die UGCP würden die Anbieter von Web 2.0-Diensten von den Rechtsinhabern zur Vornahme von Handlungen weit über die gesetzlich vorgesehenen Pflichten hinaus verpflichtet.[674] Sinn und Zweck der UGCP sei somit allein, die Last des *copyright policing* von den Rechtsinhabern auf die Anbieter von Web 2.0-Diensten überzuwälzen und damit die durch die Safe-Harbor-Regelungen geschaffene Verteilung von Rechten und Pflichten in Bezug auf die Ahndung von Urheberrechtsverletzungen im Internet faktisch außer Kraft zu setzen.[675] Weiterhin wurde als ein Schwachpunkt der UGCP identifiziert, dass sich das Unternehmen Google an der Initiative nicht beteiligt hatte. Goolges Tochterunternehmen YouTube hatte die Initiative zwar begrüßt, sich dieser aber nicht direkt angeschlossen und eine Zusammenarbeit nur im Zusammenhang mit der Fortentwicklung seiner eigenen „industrieweit führenden Werkzeuge" in Aussicht gestellt.[676] Weiterhin kam das Unternehmen der Veröffentlichung der UGCP mit der Ankündigung seiner eigenen, unternehmensintern entwickelten Content-ID-Technologie zuvor.[677] YouTubes Strategie der Entwicklung einer eigenen, proprietären Content-Identification-Technologie wurde daraufhin von den Mitinitiatoren der UGCP-Initiative scharf kritisiert, da sie

672 Vgl. Ziff. 14 UGCP.
673 *Meyers*, 26 Cardozo Arts & Entertainment L. J. 935, 945 (2009).
674 *Bangeman*, Consortium's user-generated content principles extend far beyond fair use, Ars Technica, 18.10.2007, http://arstechnica.com/news.ars/post/20071018-consortiums-user-generated-content-principles-extend-far-beyond-fair-use.html (zuletzt abgerufen am 01.07.2010).
675 *Bangeman* s.o.
676 *Heise Online*, Sorge um Nutzerrechte wegen Copyright-Filter fürs Web 2.0, 20.10.2007, http://www.heise.de/newsticker/meldung/97678 (zuletzt abgerufen am 01.07.2010).
Heise Online s.o.
677 Vgl. 7. Kapitel, Teil B.I.

deren Ziel der Entwicklung einer einheitlich für alle Web 2.0-Dienste standardisierten, nicht-proprietären Content-Identification-Technologie konterkariert.[678]

II. Pflichten von Web 2.0-Diensten im Zusammenhang mit der Durchsetzung von Urheberrechten als Gegenstand der Klage Viacom vs. YouTube

Der Umfang der den Betreibern von Internetdienten im Zusammenhang mit der Durchsetzung von Urheberrechten obliegenden Pflichten spielt zunehmend auch in den Klagen der Rechtsinhaber gegen ISPs eine Rolle. Prominentestes Beispiel hierfür ist die im März 2007 wegen „massiver" Urheberrechtsverletzungen beim District Court for the Southern District of New York erhobene Klage des Medienkonzerns Viacom International Inc. („Viacom", nachfolgend „Kläger")[679] gegen die Betreiber der Videoplattform YouTube sowie deren Mutterunternehmen Google (YouTube und Google nachfolgend gemeinsam „Beklagte").[680] Darin wird gefordert, die Beklagten dazu zu verpflichten, vernünftige Methoden („reasonable methodologies") zur Verhinderung oder Verringerung von Urheberrechtsverletzungen einzusetzen, sowie wegen bereits begangener Urheberrechtsverletzungen Schadensersatz in Höhe von mindestens US$ 1 Milliarde zu zahlen.[681] Diesen Schadensersatzanspruch stützen die Kläger auf eine unmittelbare, vorsätzliche Verletzung der durch den *Copyright Act* den Rechtsinhabern ausschließlich eingeräumten Rechte der Vervielfältigung sowie der öffentlichen Ausstellung und Aufführung und zudem auf die Verletzung ihrer Rechte nach den Grundsätzen der urheberrechtlichen Sekundärhaftung.[682] Alles in allem bedrohe die „schamlose Missachtung" des Urheberrechts durch die Beklagten nicht nur die Existenzgrund-

678 So der damalige Viacom-Chef in einer Stellungnahme auf dem Web 2.0 Summit, vgl. *Bangeman*, Viacom's true desire: one copyright filter to rule them all, Ars Technica, 22.10.2007, http://arstechnica.com/news.ars/post/20071022-viacoms-true-desire-one-copyright-filter-to-rule-them-all.html?rel (zuletzt abgerufen am 01.07.2010); *Heise Online*, Sorge um Nutzerrechte wegen Copyright-Filter fürs Web 2.0, 20.10.2007, http://www.heise.de/newsticker/meldung/97678 (zuletzt abgerufen am 01.07.2010).

679 Nach eigenen Angaben in der Klageschrift betreibt Viacom Medienunternehmen wie beispielsweise die Fernsehsender MTV und VH1 sowie die Dreamworks-Filmstudios, die Fernsehprogramme, Kinofilme, Kurzfilme und andere Unterhaltungsformate produzieren und quer durch sämtliche derzeit verfügbaren multimedialen Vertriebswege wie beispielsweise Fernsehen, Kino, DVD, Internet, Smartphones etc. vermarkten.

680 Viacom International Inc., Comedy Partners, Country Music Television, Inc., Paramount Pictures Corporation, and Black Entertainment Television LLC v. YouTube, Inc., YouTube, LLC, and Google Inc. (Defendants), Complaint for Declaratory and Injunctive Relief and Damages, 13.03.2007, U. S. District Court for the Southern District of New York, Case No. 07 CV 2103 ("Viacom Complaint"), abrufbar unter http://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1:2007cv 02103/302164/1/ (zuletzt abgerufen am 01.07.2010).

681 Viacom Complaint, S. 5.

682 Viacom Complaint, S. 18 ff.

lage der Kläger, sondern darüber hinaus allgemein die ökonomischen Grundlagen der Filmindustrie und damit „eines der wichtigsten Sektoren der Wirtschaft der Vereinigten Staaten“.[683]

1. Die Argumente der Kläger

Inhaltlich wird den Beklagten vorgeworfen, ihren Internetdienst vorsätzlich und im großen Stil zur Verletzung der Urheberrechte der Kläger zu missbrauchen, indem sie sich die von den Nutzern ohne Erlaubnis auf ihren Internetdienst hochgeladenen kreativen Inhalte der Kläger zu ihrem eigenen wirtschaftlichen Vorteil zu eigen machen würden.[684] Anders als gemeinhin angenommen sei der von den Beklagten angebotene Internetdienst nicht hauptsächlich ein Forum für urheberrechtlich unbedenkliche nutzergenerierte Inhalte, sondern bestehe dessen Angebot im Wesentlichen aus rechtswidrigen Kopien urheberrechtlich geschützter Multimediawerke. Im Zeitpunkt der Klageerhebung seien auf der Webseite mehr als 150.000 illegale Videodateien identifizierbar gewesen, die von den Nutzern der Videoplattform bereits mehr als eineinhalb milliardenmal angesehen worden seien.[685] Diese Umstände seien den Beklagten sehr wohl bewusst und Teil ihres Geschäftsplans, da der große Anteil illegal abrufbarer urheberrechtlich geschützter Multimediawerke den Marktanteil und die Attraktivität des Internetdienstes für Werbepartner steigere, und damit gleichzeitig den Wert des Unternehmens der Beklagten.[686] Damit stehen die Einkünfte der Beklagten nach Auffassung der Kläger jedoch in unmittelbarem Zusammenhang mit den durch die Nutzer begangenen Urheberrechtsverletzungen.[687]

Zudem hätten sich die Beklagten bewusst dagegen entschieden, angemessene Vorkehrungen zu treffen, um den „wildwuchsartigen“ Rechtsverletzungen auf ihrem Internetdienst Einhalt zu gebieten. Die Last, Rechtsverletzungen zu verfolgen, sei vollständig auf die Rechtsinhaber übergewälzt worden, die allein mit dem Aufwand belastet seien, den Internetdienst täglich oder gar stündlich nach rechtswidrigem Material zu durchsuchen und entsprechende Takedown-Notices an die Be-

683 Viacom Complaint, S. 2: *„Using the leverage of the Internet, YouTube appropriates the value of creative content on a massive scale for YouTube's benefit without payment or license. YouTube's brazen disregard of the intellectual property laws fundamentally threatens not just Plaintiffs, but the economic underpinnings of one of the most important sectors of the United States economy“*.
684 Viacom Complaint, s.o.
685 Viacom Complaint, S. 3.
686 Viacom Complaint, S. 3, 13.
687 Viacom Complaint, S. 13.

klagten zu senden.[688] Auch entfernten die Beklagten nach Erhalt einer Takedown-Notice nur die darin mit einer konkreten URL-Adresse aufgelisteten Videodateien, nicht hingegen identische Dateien, die unter anderen Adressen auf dem Internetdienst vorhanden seien. Daher sei als rechtswidrig angezeigtes und daraufhin von der Webseite heruntergenommenes Material in vielen Fällen unter anderen Adressen weiterhin auf dem Internetdienst abrufbar oder werde innerhalb von wenigen Stunden von anderen Nutzern erneut auf den Dienst hochgeladen.[689]

Auch die von den Beklagten zur Verfügung gestellten Werkzeuge zur Beseitigung rechtswidrigen Materials seien keine Hilfe, da sie allenfalls dazu beitragen könnten, einen Teil der rechtswidrigen Videodateien aufzufinden, und dies auch erst dann, wenn die Inhalte bereits auf den Internetdienst hochgeladen worden seien.[690] Diese Werkzeuge würden von den Beklagten zwar dazu eingesetzt, um das Hochladen von Videodateien, deren Inhalte mit urheberrechtlich geschützten Inhalten identisch sind, zu verhindern, jedoch seien sie nicht in der Lage, solche Dateien auch dann zu erkennen, wenn an ihnen geringfügige Änderungen vorgenommen worden seien.[691] Darüber hinaus würden die von den Beklagten zur Identifikation von Urheberrechtsverletzungen eingesetzten Filtertechnologien als Druckmittel benutzt, um die Rechtsinhaber dazu zu zwingen, ihnen Lizenzen zur Nutzung ihrer urheberrechtlich geschützten Multimediawerke im Rahmen der Videoplattform zu gewähren, da die Filtertechnologien nur zum Schutz derjenigen Rechtsinhaber eingesetzt würden, die mit den Beklagten eine entsprechende vertragliche Vereinbarung abgeschlossen haben.[692] Hierzu ist anzumerken, dass sich die technischen Parameter der Instrumente, die von YouTube zum Schutz urheberrechtlich geschützter Multimediawerke angeboten werden, seit Erhebung der Klage stark verändert haben, vor allem durch die Einführung der Content-ID-Technologie im Oktober 2007.[693]

688 Viacom Complaint, S. 3, 15; Viacom beschäftigt nach eigenen Angaben ein bis zwei Dutzend Angestellte ständig damit, die auf YouTube hochgeladenen Videos auf Urheberrechtsverletzungen hin zu überprüfen, wobei davon auszugehen ist, dass ein Mitarbeiter zwischen 40 und 50 Videos in der Stunde abarbeiten kann, vgl. *Steinert-Threlkeld*, YouTube's video ID system: is 75 percent good enough?, in: ZDNet Undercover: YouTube's Video Identification System, November 2008, S. 3.

689 Viacom Complaint, S. 4.

690 Viacom Complaint, S. 15.

691 Viacom Complaint, S. 15.

692 Viacom Complaint, S. 4, 17; Ausweislich der Beschreibung der Audio-ID- und Video-ID-Technologie auf YouTube steht dieses Tool ausdrücklich jedem Rechtsinhaber, d.h. nicht nur YouTubes offiziellen (Vertrags-) Partnern zur Verfügung. Voraussetzung ist lediglich, dass der Rechtsinhaber YouTube entsprechende Informationen über die zu schützenden Inhalte zur Verfügung stellt, damit die Filtertechnologien rechtswidriges Material auf dieser Grundlage aufspüren können, vgl. hierzu 8. Kapitel, Teil B.III.4.f.

693 Vgl. 7. Kapitel, Teil B.IV.

2. Die Verteidigung der Beklagten

Ihre Verteidigung stützen die Beklagten in erster Linie auf die Safe-Harbor-Regelung gemäß § 512(c).[694] Deren Voraussetzungen würden die Beklagten nicht nur erfüllen, sondern darüber hinaus in Form zusätzlicher Verfahren zum Schutz von Urheberrechten, wie beispielsweise dem Programm zur Inhaltsprüfung sowie der automatisierten Takedown-Notice den Rechtsinhabern ein Schutzniveau bieten, das weit über das gesetzlich Erforderliche hinausgehe.[695] Das Begehren und die Argumentation der Kläger stelle somit den in der Haftungsbeschränkung niedergelegten, vom Gesetzgeber mit Bedacht austarierten Interessenausgleich zwischen Host-Providern und Rechtsinhabern grundsätzlich in Frage und bedrohe damit den ungehinderten Informationsaustausch über das Internet in der Form, wie er derzeit von Millionen von Menschen praktiziert werde.[696]

B. Die Haftung von Web 2.0-Diensten für Urheberrechtsverletzungen der Nutzer ihrer Internetdienste nach US-amerikanischem Urheberrecht

Fraglich ist, ob sich die Forderung der Rechtsinhaber nach einer größeren Beteiligung der Betreiber von Web 2.0-Diensten am *copyright policing* durch den Einsatz von Content-Identification-Technologien im Rahmen ihrer Internetdienste auch rechtlich begründen lässt. Um diese Frage beantworten zu können, werden nachfolgend zunächst die Rahmenbedingungen der Haftung von ISPs nach US-amerikanischem Urheberrecht, insbesondere die Haftungsregelungen der urheberrechtlichen Sekundärhaftung und die Haftungsbeschränkung für Host-Provider gemäß 17 U.S.C. § 512(c), dargestellt und auf dieser Grundlage die rechtliche Begründbarkeit der Forderung nach einem verstärkten Einsatz von Content-Identification-Technologien durch ISPs geprüft. Im Anschluss daran wird dieselbe Frage nach

694 Vgl. Viacom International Inc., et al. v. YouTube, Inc., et al., Defendant's Answer and Demand for Jury Trial, 30.04.2007, Case No. 1:07-cv-02103 (LLS) (FM) („YouTube Answer"), S. 10, abrufbar unter http://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1:2007cv 02103/302164/21/0.pdf (abgerufen am 13.10.2009).

695 Vgl. YouTube Answer, S. 1.

696 YouTube Answer s.o.: *„Viacom's complaint in this action challenges the careful balance established by Congress when it enacted the Digital Millennium Copyright Act. The DMCA balances the rights of copyright holders and the need to protect the internet as an important new form of communication. By seeking to make carriers and hosting providers liable for internet communications, Viacom's complaint threatens the way hundreds of millions of people legitimately exchange information, news, entertainment, and political and artistic expression"*.

deutsch-europäischem Recht geprüft und die Ergebnisse dieser Analyse denjenigen des US-amerikanischen Rechts gegenübergestellt.

I. Primary liability

Zu prüfen ist zunächst eine Haftung der Betreiber von Web 2.0-Diensten wegen einer unmittelbaren Verletzung des *copyright* an Multimediawerken durch Material, das von den Nutzern rechtswidrig in diese Dienste eingestellt wird, unter Berücksichtigung der Verfügbarkeit von Content-Identification-Technologien.

1. Schutzgegenstand

Gemäß 17 U.S.C. § 102(a) gibt es acht Kategorien schutzfähiger Werkarten, darunter Filme und andere audiovisuelle Werke sowie Tonaufnahmen.

„Audiovisuelle Werke" werden in 17 U.S.C. § 101 legaldefinert als Werke, die aus einer Abfolge miteinander verbundener Bilder bestehen und die dazu bestimmt sind, mit Hilfe von Maschinen oder Gerätschaften - wie beispielsweise Projektoren - gemeinsam mit den beigefügten Tonfolgen gezeigt bzw. abgespielt zu werden. Darüber hinaus werden „Filme" definiert als audiovisuelle Werke, die aus einer Abfolge miteinander verbundener Bilder bestehen, die bei ihrem Abspielen den Eindruck einer Bewegung hervorrufen.[697] Die in einem audiovisuellen Werk verkörperten Bilder, literarischen Werke und/oder Musikwerke werden als Teil des audiovisuellen Werks geschützt, auch wenn sie – jeweils für sich genommen – den Schutz einer anderen Werkkategorie für sich beanspruchen könnten.[698] Dies gilt insbesondere für die einem audiovisuellen Werk beigefügten Töne, so dass der Soundtrack zu einem Film grundsätzlich als Teil des Filmwerks geschützt wird.[699]

Auch Tonaufnahmen genießen urheberrechtlichen Schutz.[700] Gemäß 17 U.S.C. § 101 sind unter dem Begriff der Tonaufnahme Werke zu verstehen, die aus der Fixierung einer Abfolge von musikalischen, gesprochenen oder anderen Tönen bestehen. Entsprechend dem Grundsatz, dass Tonfolgen, die einem audiovisuellen Werk beigefügt sind, ausschließlich als dessen Teil geschützt werden, erfasst dieser Begriff nicht Tonfolgen, die in einem Film oder einem anderen audiovisuellen Werk enthalten sind. Von der Tonaufnahme zu unterscheiden ist das Musikwerk oder das literarische Werk, auf dem es basiert und die ebenfalls urheberrechtlich

697 *Nimmer*, in: Nimmer on Copyright, 2009, 2009, § 2.9[C], 2-152.
698 *Goldstein*, Copyright, 2005, § 2.12, 2:139; *Nimmer*, in: Nimmer on Copyright, 2009, 2009, § 2.9[B], 2-150, 2-151.
699 *Goldstein* s.o.
700 *Goldstein*, Copyright, 2005, § 2.13, 2:146-47.

geschützt sind.[701] Grundsätzlich bedarf somit derjenige, der ein musikalisches oder literarisches Werk wiedergeben und aufnehmen will, der Zustimmung des jeweiligen Rechtsinhabers hierzu. Eine Ausnahme gilt für sogenannte „nondramatic musical compositions", für die das Gesetz in 17 U.S.C. § 115 eine Zwangslizenz vorsieht.[702]

Wie eingangs dargestellt wurde, bestehen Multimediawerke aus Musikwerken, Tonaufnahmen oder Filmwerken bzw. Kombinationen dieser Ausdrucksformen. Da sowohl Filme als auch Tonaufnahmen nach US-amerikanischem Urheberrecht schutzfähig sind, genießen Multimediawerke, die in Web 2.0-Dienste eingestellt werden, grundsätzlich Schutz durch das US-amerikanische *copyright law*.

2. Unmittelbare Rechtsverletzung

Wie bereits dargelegt wurde, liegt eine unmittelbare Rechtsverletzung eines Werks gemäß 17 U.S.C. § 501(a) vor, wenn eines der dem Rechtsinhaber durch das *copyright* ausschließlich gewährten Verwertungsrechte ohne dessen Erlaubnis ausgeübt wird.[703] Im Zusammenhang mit Rechtsverletzungen, die im Rahmen von Web 2.0-Diensten an urheberrechtlich geschützten Multimediawerken begangen werden, kommt vor allem ein Eingriff in das Vervielfältigungsrecht, das Verbreitungsrecht sowie das Recht auf öffentliche Aufführung in Betracht.

a. Vervielfältigungsrecht

Der Inhaber eines *copyright* hat gemäß 17 U.S.C. § 106(1) das ausschließliche Recht, sein Werk in Form von Kopien oder Tonträger zu vervielfältigen. Durch den Begriff der Vervielfältigung wird dieses Recht zum einen vom Verbreitungsrecht gemäß 17 U.S.C. § 106(3) abgegrenzt, das implizit voraussetzt, dass ein Vervielfältigungsstück bereits vorliegt; auch ist für die Verletzung des Vervielfältigungsrechts nicht Voraussetzung, dass die Kopie des geschützten Werks anschließend auch an Dritte weiterverbreitet wird.[704] Zum anderen setzt weder das Ausstellungs- noch das Aufführungsrecht gemäß 17 U.S.C. §§ 106(4), 106(5) voraus, dass von dem Werk ein Vervielfältigungsstück angefertigt wird.[705] Kopien werden in 17 U.S.C. § 101 gesetzlich definiert als „materielle Objekte", durch die

701 *Goldstein*, Copyright, 2005, § 2.13, 2:147-48; *Nimmer*, in: Nimmer on Copyright, 2009, 2009, § 2.10[A], 2-172.1.
702 *Goldstein*, Copyright, 2005, § 2.13, 2:148.
703 Vgl. 5. Kapitel, Teil B.III.1.a.
704 *Nimmer*, in: Nimmer on Copyright, 2009, § 8.02, 8-30.
705 *Nimmer* s.o; *Goldstein*, Copyright, 2005, § 7.1, 7:12.

ein Werk in irgendeiner Weise festgehalten wird, so dass es hierdurch entweder unmittelbar oder mit Hilfe entsprechender Gerätschaften wahrgenommen, vervielfältigt oder anderweitig kommuniziert werden kann.[706] Unter den Begriff des Tonträgers fallen materielle Objekte, durch die Töne oder Tonfolgen, die nicht Teil eines audiovisuellen Werks oder Films sind, festgehalten werden können.[707] Für den rechtswidrigen Eingriff in das Vervielfältigungsrecht spielt es keine Rolle, in welchem Umfang und auf welche Art und Weise eine Kopie des Werks hergestellt wird. Es ist somit nicht erforderlich, dass von dem gesamten Werk eine identische Kopie in gleicher Werkgattung angefertigt wird.[708]

So wird für eine Verletzung des Vervielfältigungsrechts beispielsweise als ausreichend angesehen, wenn ein geschütztes Computerprogramm in den Arbeitsspeicher des Computers eines Nutzers kopiert wird.[709] Eine Verletzung des Vervielfältigungsrechts stellt auch das Hochladen von Fotografien auf eine Webseite ohne Erlaubnis des Rechtsinhabers dar,[710] wenn hierdurch eine digitale Kopie des Werks auf dem Server des Internetdienstes gespeichert wird.[711] Weiterhin liegt ein Eingriff in das Vervielfältigungsrecht vor, wenn ein geschütztes Werk auf den Computer des Nutzers heruntergeladen und dort gespeichert wird.[712] Stellt somit ein Nutzer ein durch ein *copyright* geschütztes Multimediawerk auf einem Web 2.0-Dienst ein, lieg in der hierdurch veranlassten Speicherung einer Kopie des Multimediawerks auf dem Server des Dienstes eine Verletzung des Vervielfältigungsrechts des Rechtsinhabers.

b. Verbreitungsrecht

Gemäß 17 U.S.C. § 106(3) ist auch nur der Rechtsinhaber berechtigt, Kopien oder Tonträger des geschützten Werks an die Öffentlichkeit zu verbreiten, beispielsweise im Wege des Verkaufs oder der anderweitigen Übertragung des Eigentums, der Miete oder der Leihe. Der Rechtsinhaber ist der einzige, der eine materielle

706 *"Copies are material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.".*

707 *"Phonorecords are material objects, in which sounds, other than those accompanying a motion picture or other audiovisual work, are fixed by any method now known or later developed… .".*

708 *Merges/Menell/Lemley*, Intellectual Property, 2003, S. 403; *Nimmer*, in: Nimmer on Copyright, 2009, § 8.02[D], 8-34.1.

709 *Goldstein*, Copyright, 2005, § 7.1, 7:12-713.

710 *Paisley Park Enterprises, Inc. v. Uptown Productions*, 54 F. Supp2 d 347 (S.D.N.Y. 1999); *Ross*, IP Law, 2000, § 6.02[1], 6-9.

711 *von Rosenberg*, K&R 1999, 402.

712 *MAI Systems Corp. V. Peak Computer, Inc.*, 991 F.2 d 511 (9th Cir. 1993); *Ross*, IP Law, 2000, § 6.02[1], 6-9.

Verkörperung seines Werks verkaufen, vermieten oder verleihen darf.[713] 17 U.S.C. § 106(3) enthält somit das Recht zur ersten Veröffentlichung.[714] „Öffentlich" ist die Verbreitung, wenn die Vervielfältigungsstücke einer unbegrenzten Anzahl von Personen zur Verfügung gestellt werden, wobei es keine Rolle spielt, ob die Verbreitung abhängig von einer Gegenleistung erfolgt.[715]

Das Verbreitungsrecht ist beispielsweise dann betroffen, wenn Kopien eines digitalen Multimediawerks in Form von Downloads über das Internet an einen unbegrenzten Kreis Dritter ausgeliefert werden, wie dies regelmäßig im Rahmen eines Filesharing-Netzwerks der Fall ist.[716] Weniger eindeutig ist der Eingriff in das Verbreitungsrecht hingegen im Kontext von Web 2.0-Diensten, da hier der Nutzer digitale Multimediawerke in der Regel nicht unmittelbar an Dritte verbreitet. Vielmehr werden diese zunächst „nur" auf dem Server des Internetdienstes gespeichert, um im Anschluss daran von Dritten abgerufen und gegebenenfalls auch heruntergeladen werden zu können, wobei letzteres nur möglich ist, wenn der ISP hierfür eigens eine entsprechende Funktion zur Verfügung stellt. Ob jedoch die bloße Einräumung der Möglichkeit zum Herunterladen, die von Dritten nicht notwendigerweise genutzt werden muss, bereits eine Verletzung des Verbreitungsrechts darstellt, ist im US-amerikanischen Recht bisher noch nicht abschließend geklärt.[717]

c. Recht der öffentlichen Aufführung

Der Rechtsinhaber ist zudem gemäß 17 U.S.C. § 106(4) allein berechtigt, das durch ein *copyright* geschützte Werk öffentlich aufzuführen. Allerdings wird dieses Recht grundsätzlich nicht in Bezug auf Tonaufnahmen gewährt. Bei dieser Werkskategorie besteht das Aufführungsrecht gemäß 17 U.S.C. § 106(6) nur, soweit es sich um eine digitale Übertragung der Tonaufnahme handelt (sogenannte „digital audio transmission"); Aufführungen, die in einer analogen Übertragung der Tonaufnahme bestehen, werden somit nicht geschützt.[718]

713 *Nimmer*, in: Nimmer on Copyright, 2009, § 8.11, 8-148.
714 *Goldstein*, Copyright, 2005, § 7.5, 7:122.1.
715 *von Rosenberg*, K&R 1999, 402.
716 *Marobie-FL. Inc. v. National Association of the Fire Equipment Distributors and Northwest Nexus, Inc.,* 983 F.Supp. 1167 (N.D. Ill. 1997); *Ginsburg*, 50 Ariz. L. Rev. 577, Fn. 1; *Ross*, IP Law, 2000, § 6.02[1], 6-9.
717 *Ginsburg* s.o.; eine Verletzung des Verbreitungsrechts durch solche Handlungen bejaht *Ross*, IP Law, 2000, § 6.02[1], 6-9.
718 Zu den politischen Hintergründen dieses eingeschränkten Schutzes für Tonaufanhmen vgl. *Goldstein*, Copyright, 2005, § 7.7, 7:152-54; *Nimmer*, in: Nimmer on Copyright, 2009, §§ 8.21 – 8.24; *Merges/Menell/Lemley*, Intellectual Property, 2003, S. 438, 440, 49.

Eine Aufführung ist immer dann gegeben, wenn ein Werk für die Zuseher bzw. Zuhörer durch einen physischen Akt wahrnehmbar gemacht wird.[719] Die Aufführung ist weiterhin „öffentlich", wenn sie entweder an einem Ort stattfindet, der der Öffentlichkeit frei zugänglich ist oder an dem sich eine über einen durchschnittlichen Familien- und Bekanntenkreis wesentlich hinausgehende Anzahl von Personen aufhält, oder wenn sie an einen solchen Ort oder generell an die Öffentlichkeit übertragen wird. Hierbei spielt keine Rolle, wo sich die Angehörigen der Öffentlichkeit zum Zeitpunkt der Übertragung aufhalten und ob die Übertragung an sie gleichzeitig oder zu unterschiedlichen Zeiten erfolgt.[720]

Im Kontext von Web 2.0-Diensten ist dieses Recht somit beispielsweise dann betroffen, wenn ein digitales Multimediawerk durch einen Nutzer in Form eines *streams* zur Verfügung gestellt wird, so dass es daraufhin auf dem Web 2.0-Dienst von einem unbegrenzten Personenkreis zu Zeiten und an Orten ihrer Wahl abgerufen werden kann.[721] Hingegen stellt das Herunterladen eines geschützten Multimediawerks keinen Eingriff in das Aufführungsrecht dar.[722]

d. Ein separates „right of making available" nach US-amerikanischem Urheberrecht?

Über die vorgenannten Rechte hinaus kennt das US-amerikanische Urheberrecht kein spezielles Recht zur öffentlichen Zugänglichmachung im Sinne eines „right of making available", wie es in Art. 8 des WIPO-Urheberrechtsvertrages ausdrücklich vorgesehen ist.[723]

e. Ergebnis

Lädt ein Nutzer ein durch ein *copyright* geschütztes Multimediawerk auf einen Web 2.0-Dienst hoch, ohne dass der Rechtsinhaber hierin eingewilligt hat, liegt darin eine Verletzung des Vervielfältigungsrechts sowie des Rechts der öffentlichen Aufführung. Haben die Nutzer zudem die Möglichkeit, eine Kopie des Mul-

719 *Merges/Menell/Lemley*, Intellectual Property, 2003, S. 438 f.
720 Vgl. 17 U.S.C. § 101.
721 *United States of America v. American Society of Composers, Authors and Publishers*, 485 F. Supp. 2 d 438, 443-44 (S.D.N.Y. 2007); *Ginsburg*, 50 Ariz. L. Rev. 577, Fn. 1.
722 485 F. Supp. 2 d 438, 444.
723 *Ginsburg*, 50 Ariz. L. Rev. 577, Fn. 1; vgl. weiterführend *Ginsburg*, The (new?) Right of Making Available to the Public, 2004, abrufbar unter http://ssrn.com/abstract=602623 (zuletzt abgerufen am 01.07.2010).

timediawerks auf ihre Computer herunterzuladen, wird hierdurch auch in das Verbreitungsrecht eingegriffen.

3. Zurechnung der Rechtsverletzungen der Nutzer an den ISP

Über die Frage der Rechtsverletzung hinaus stellt sich die Frage nach der Zurechenbarkeit dieser Rechtsverletzung, die unmittelbar durch die Nutzer der Web 2.0-Dienste begangen wird, an den ISP, der den Dienst betreibt. Die Rechtsprechung der US-amerikanischen Gerichte zu dieser Frage ist uneinheitlich.[724] Die beiden einflussreichsten Entscheidungen in diesem Zusammenhang werden nachfolgend kurz dargestellt.

a. Playboy Enterprises, Inc. v. Frena

Gegenstand des Verfahrens *Playboy Enterprises, Inc. v. Frena*[725] („Frena") war eine Klage des Herausgebers des Magazins „Playboy" („Kläger") gegen George Frena („Beklagter"), den Betreiber eines kostenpflichtigen Internetforums namens „Techs Warehouse BBS". Die Nutzer des Forums konnten hierauf Informationen und digitale Inhalte wie beispielsweise Fotografien einstellen, so dass andere Nutzer darauf zugreifen und sie auf ihre Computer herunterladen konnten. Ohne dass der Beklagte hiervon wusste, befanden sich auf dem Forum zeitweise auch einige Kopien von urheberrechtlich geschützten Fotografien, an denen der Kläger Rechte hielt und die ohne dessen Einwilligung auf dem Forum eingestellt worden waren. Nachdem der Kläger den Beklagten hierüber informiert hatte, wurden die Fotografien vom Beklagten entfernt. Auch überwachte der Beklagte fortan seinen Internetdienst, um das erneute Hochladen von Kopien der Fotografien des Klägers zu verhindern. Dennoch verurteilte das Gericht den Beklagten wegen einer unmittelbaren Verletzung der Rechte des Klägers in Bezug auf die Verbreitung und öffentlichen Ausstellung der Fotografien des Klägers. Die Haftung des Beklagten stützte das Gericht darauf, dass der Beklagte ein Produkt in Form des Internetforums vertrieben habe, das rechtswidrige Kopien der urheberrechtlich geschützten

724 Vgl. *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993); *Sega Enterprises Ltd. v. Maphia*, 857 F. Supp. 679, 683 (N.D. Cal. 1994); *MAI Systems Corporation v. Peak Computer Inc*., 991 F.2 d 511 (9th Circuit 1993); *Religious Technology Ctr. v. Netcom On-Line Comm. Servs., Inc.*, 907 F. Supp. 1361 (N.D. Cal 1995); *Marobie-FL, Inc. v. Nat. Assn. of Fire Equip. Distribs. and Northwest Nexus, Inc.*, 983 F. Supp. 1167 (N.D. Ill. 1997); *Playboy Enters., Inc. v. Webbworld, Inc.*, 968 F. Supp. 1171 (N.D. Tex. 1997); *Playboy Enters., Inc. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503 (N.D. Ohio 1997); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2 d 1146 (C.D. Cal. 1998).

725 *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993).

Werke des Klägers enthalten habe. Nach Auffassung des Gerichts war für die Haftung des Beklagten ohne Bedeutung, dass diese rechtswidrigen Kopien nicht vom Beklagten, sondern von den Nutzern in das vom Beklagten vertriebene „Produkt" eingebracht worden waren.[726]

Diese Entscheidung wird aus mehreren Gründen kritisiert. Zunächst ist für eine unmittelbare Verletzung des Verbreitungsrechts grundsätzlich erforderlich, dass der Rechtsverletzer selbst eine rechtswidrige materielle Verkörperung eines urheberrechtlich geschützten Werks vertreibt.[727] In *Frena* bestand jedoch die einzige unmittelbare Handlung des Beklagten, auf die seine Haftung gestützt werden konnte, in der Erbringung einer Dienstleistung, nämlich der Zurverfügungstellung und der Unterhaltung des Internetforums. Das einzige Produkt, das somit vom Beklagten vertrieben wurde, war die Möglichkeit der Nutzung des Internetforums, nicht hingegen eine rechtswidrig erstellte Verkörperung eines urheberrechtlich geschützten Werks.

Weiterhin hätte im Rahmen der Prüfung einer unmittelbaren Verletzung des Rechts auf öffentliche Ausstellung geklärt werden müssen, ob die Ausstellung der Fotografien im Forum dem Beklagten als eigene Handlung zugerechnet werden konnte oder ausschließlich dem die Ausstellung unmittelbar veranlassenden Nutzer.[728] Denn wenn die Handlung dem Beklagten nicht zugerechnet werden kann, kommt seinerseits eine Haftung nur nach den Grundsätzen der Sekundärhaftung[729] und den insoweit geltenden besonderen Voraussetzungen in Frage.[730]

b. Religious Technology Center v. Netcom On-Line Communication Services, Inc.

Zu einem völlig anderen Ergebnis in Bezug auf die Zurechnung von Nutzerhandlungen an einen ISP kam das Gericht in *Religious Technology Center v. Netcom*

726 839 F. Supp. 1552, 1556: *„There is no dispute that Defendant Frena supplied a product containing unauthorized copies of a copyrighted work. It does not matter that Defendant Frena claims he did not make the copies itself."*.

727 *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.01[A][1], S. 12B-6.

728 Vgl. beispielsweise *Religious Technology Center v. Netcom On-Line Communication Services*, *Inc.*, 907 F. Supp. 1361, 1372 (N.D. Cal. 1995): *"Playboy concluded that the defendant infringed the plaintiff's exclusive rights to publicly distribute and display copies of its works. … The court is not entirely convinced that the mere possession of a digital copy on a BBS that is accessible to some members of the public constitutes direct infringement by the BBS operator. Such a holding suffers from the same problem of causation as the reproduction argument. Only the subscriber should be liable for causing the distribution of plaintiffs' work, as the contributing actions of the BBS provider are automatic and indiscriminate."*.

729 Vgl. 8. Kapitel, Teil B.II.

730 *Nimmer* in: Nimmer on Copyright, 2009, § 12B.01[A][1], S. 12B-7.

On-Line Communication Services, Inc. ("Netcom").[731] In diesem Fall ging es um die Haftung eines großen Access-Providers („Beklagter") für über das Internet verbreitete Äußerungen des Nutzers eines Usenet-Netzwerks („Usenet").[732]

Ausgangspunkt des Rechtsstreits waren wörtliche Zitate aus Veröffentlichungen des Scientology-Gründers L. Ron Hubbard, die ein ehemaliges Scientology-Mitglied („Usenet-Nutzer") zusammen mit einigen kritischen Anmerkungen hierzu über ein Usenet verbreitet hatte. Das Gericht hatte in einem ersten Verfahren gegen den Usenet-Nutzer festgestellt, dass dieser durch sein Verhalten die Urheberrechte des Verlags („Kläger") an diesen Veröffentlichungen verletzt hatte und seine Handlungen auch nicht nach den Grundsätzen der Fair-Use-Doktrin gerechtfertigt waren.[733] In *Netcom* ging es nunmehr um die Frage, ob neben dem Usenet-Nutzer auch der beklagte Access-Provider für die Urheberrechtsverletzungen haftete. Denn die Zitate waren in einem automatisierten Verfahren vom Computer des Nutzers auf die Server des Beklagten kopiert und von dort aus im Internet weiterverbreitet worden.[734]

Vor diesem Hintergrund stellte das Gericht fest, dass die Vervielfältigung der Zitate des Usenet-Nutzers auf den Servern des Beklagten im Rahmen des routinemäßigen, durch die Software des Beklagten automatisiert gesteuerten technischen Prozesses zur Weiterleitung von Mitteilungen aus Usenet-Netzwerken keine unmittelbare Verletzung des Vervielfältigungsrechts des Klägers darstellte.[735] Nach Auffassung des Gerichts scheiterte die Haftung daran, dass seitens des Beklagten keine „affirmative action" vorlag, d.h. kein Verhalten, durch das die von dem Usenet-Nutzer unmittelbar begangene Urheberrechtsverletzung vertieft worden war. Denn die einzige Verbindung des Beklagten zu dem rechtswidrigen Verhalten des Usenet-Nutzers bestand in einem durch die Software automatisiert ausgelösten, ohne jegliche menschliche Mitwirkung ausgeführten Vervielfältigungsakt, der un-

731 *Religious Technology Center v. Netcom On-Line Communication Services*, *Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995).

732 Für eine Erklärung des Begriffes „Usenet" vgl. *Ellison v. Robertson*, 189 F. Supp. 2 d 1051, 1053-54 (C.D. Cal. 2002): *„The USENET, an abbreviation of "User Network," is an international collection of organizations and individuals (known as 'peers') whose computers connect to each other and exchange messages posted by USENET users. Messages are organized into "newsgroups," which are topic-based discussion forums where individuals exchange ideas and information. Users' messages may contain the users' analyses and opinions, copies of newspaper or magazine articles, and even binary files containing binary copies of musical and literary works. ... Peers in USENET enter into peer agreements, whereby one peer's servers automatically transmit and receive newsgroup messages from another peer's servers. As most peers are parties to a large number of peer agreements, messages posted on one USENET peer's server are quickly transmitted around the world. The result is a huge informational exchange system whereby millions of users can exchange millions of messages every day."*

733 907 F. Supp. 1361, Fn. 3.

734 907 F. Supp. 1361, 1365.

735 907 F. Supp. 1361, 1368-71.

abhängig vom Inhalt der auf einem Usenet eingestellten Mitteilung („posting") immer nach dem gleichen Schema ablief, wenn ein neues *posting* in einem Usenet-Netzwerk veröffentlicht wurde. Über diesen automatisierten Prozess hinaus war nach Dafürhalten des Gerichts jedoch zur Begründung einer Haftung des Beklagten ein gewisses Maß an Willentlichkeit („volition") oder Ursächlichkeit („causation") zu verlangen, da ansonsten jeder Nutzer eines Computers, der als ein Usenet-Server fungiert und über den *postings* weiterverbreitet werden, für die Rechtswidrigkeit dieser *postings* haften würde. Dadurch würde aber die Funktionsfähigkeit von Usenet-Diensten generell in Frage gestellt. Eine solche unerwünschte Ausuferung der Haftung für Urheberrechtsverletzungen im Internet müsse vermieden werden.

Auch verneinte das Gericht die Haftung des Beklagten wegen einer unmittelbaren Verletzung des Verbreitungsrechts sowie des Rechts auf öffentliche Ausstellung des Klägers und wich damit ausdrücklich von der Rechtsauffassung des Gerichts in *Frena* ab.[736] Wiederum begründete das Gericht seine Entscheidung insoweit mit dem Fehlen eines über den standardmäßigen, automatisierten Ablauf der Verbreitung eines *postings* hinausgehenden Akts und damit mit dem Fehlen von *volition* oder *causation* in Bezug auf die durch die Nutzer begangenen Urheberrechtsverletzungen. Dabei spielte für das Gericht auch eine Rolle, dass es für den Beklagten praktisch nicht möglich war, die tagtäglich innerhalb seiner Netzinfrastruktur übermittelten „billions of bits of data" auf die Rechtmäßigkeit der darin verkörperten digitalen Inhalte zu überprüfen, d.h. „infringing bits from noninfringing bits" zu unterscheiden und auszusortieren.[737]

c. Rechtslage post-DMCA

An der Widersprüchlichkeit dieser Entscheidungen wird die Rechtsunsicherheit deutlich, der sich ISPs in Bezug auf ihre Haftung für Urheberrechtsverletzungen der Nutzer ihrer Internetdienste zwischenzeitlich ausgesetzt sahen. Diese Rechtunsicherheit beabsichtigte der US-amerikanische Gesetzgeber durch Einführung der Haftungsbeschränkung gemäß 17 U.S.C § 512 zu beseitigen. Zu diesem Zweck war zunächst geplant, die tragenden Erwägungen des Gerichts in *Netcom* zu kodifizieren:

> „As to direct infringement, liability is ruled out for passive automatic acts engaged in through a technological process initiated by another. Thus, the bill essentially codifies the result in the leading and most toughtful judicial decision to date: Religious Technology Center v. Netcom On-line Communications

736 907 F. Supp. 1361, 1372.
737 907 F. Supp. 1361, 1372-73.

> Services, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995). In doing so it overrules those aspects of Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993), insofar as the case suggests that such acts by service providers could constitute direct infringement, and provides certainty that Netcom and its progeny ... will be the law of the land."[738]

Zwar kam der Gesetzgeber im Laufe des Gesetzgebungsvorhabens von diesem Ansatz ab und entschied sich anstattdessen, im Rahmen von 17 U.S.C. § 512 nur die Folgen der Haftung von ISPs in bestimmten Fallkonstellationen zu begrenzen. Das bereits bestehende *case law* in Bezug auf die Beurteilung der Haftung von ISPs blieb hiervon unberührt.[739] Viele Gerichte sowie Teile der Literatur gehen dennoch davon aus, dass nunmehr für die Beurteilung der Haftung von ISPs die Entscheidung *Netcom* und nicht *Frena* maßgeblich ist.[740] Dabei ist der Second Circuit in seiner Entscheidung *The Cartoon Network LP, LLLP v. CSC Holdings, Inc.* sogar so weit gegangen, den in *Netcom* entwickelten Ansatz, die unmittelbare Haftung über das Erfordernis des „volitional element" einzugrenzen, auch für Sachverhalte außerhalb des Internets heranzuziehen.[741]

Für die unmittelbare Haftung von ISPs gilt daher der Grundsatz, dass eine durch einen Nutzer begangene Urheberrechtsverletzung einem ISP nicht zugerechnet werden kann, wenn dessen Beitrag hierzu lediglich in einem durch das System oder Netzwerk des ISPs automatisiert ausgeführten technischen Vorgang besteht, dessen Auslösung allein der Willensentscheidung des jeweiligen Nutzers unterliegt. Anders gewendet scheidet eine Haftung des ISP als *direct infringer* aus, wenn seinerseits kein „volitional element" oder eine „affirmative action" in Bezug auf die Begehung der Urheberrechtsverletzung durch den Nutzer erkennbar ist.

738 H.R. Rep. 105-551 (I), S. 11.

739 Vgl. 8. Kapitel, Teil B.III.3.a.

740 Vgl. z.B. *CoStar Group Inc. v. Loopnet, Inc.*, 373 F.3 d 544, 551 (4th Cir. 2004); *Ellison v. Robertson*, 189 F. Supp. 2 d 1051, 1055 (C.D. Cal. 2002); *Perfect 10, Inc. v. Cybernet Ventures, Inc.,* 213 F. Supp. 2 d 1146, 1168-69 (C.D. Cal. 2002); *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.01[A][1], S. 12B-14, 15; *Patry*, in: Patry on Copyright, 2010, § 9:50, 9-23.

741 Vgl. *Cartoon Network LP, LLLP v. CSC Holdings, Inc.,* 536 F.3 d 121, 131 (2nd Cir. 2008): *"While the* Netcom *court was plainly concerned with a theory of direct liability that would effectively "hold the entire Internet liable" for the conduct of a single user ..., its reasonings and conclusions, consistent with precedents of this court and the Supreme Court, and with the text of the Copyright Act, transcend the Internet. ... [W]e reject the contention that "the* Netcom *decision was driven by expedience and that its holding is inconsistent with the established law of copyright"... and we find it "a particular rational interpretation of § 106", ... rather than a special-purpose rule applicable only to ISPs."*

4. Ergebnis

Ausgehend von *Netcom* ist grundsätzlich nicht anzunehmen, dass der Betreiber eines Web 2.0-Dienstes wegen der Urheberrechtsverletzungen, die seine Nutzer im Zusammenhang mit der Nutzung des Internetdienstes begehen, als *primary infringer* verurteilt werden würde.[742] Denn das Speichern einer durch einen Nutzer hochgeladenen Datei auf dem Server eines Web 2.0-Dienstes, wodurch das in der Datei verkörperte digitale Multimediawerk für andere Nutzer des Dienstes zugänglich wird, stellt einen rein automatisierten Prozess dar, der allein durch den jeweiligen Nutzer ausgelöst und gesteuert wird. Über diesen automatisierten, von einer Software ausgeführten Prozess hinaus, der in identischer Form immer dann abläuft, wenn ein Nutzer eine Datei auf einen Web 2.0-Dienst hochlädt, nimmt der jeweilige ISP in der Regel jedoch keine weiteren Handlungen vor, aufgrund derer auf eine willentliche Unterstützung der rechtswidrigen Handlungen der Nutzer im Sinne von *Netcom* geschlossen werden könnte. Da ein Web 2.0-Dienst daher bereits aus diesem Grund regelmäßig nicht als *primary infringer* haftet, stellt sich die Frage der Auswirkungen von Content-Identification-Technologien auf die (nichtexistente) unmittelbare Haftung von ISPs von vornherein nicht.

II. Secondary liability

Weiterhin stellt sich die Frage, ob ein Web 2.0-Dienst nach den Grundsätzen der Sekundärhaftung des US-amerikanischen *copyright law* für die Rechtsverletzungen der Nutzer seines Internetdienstes haftet.

1. Die Sekundärhaftung im US-amerikanischen Urheberrecht

Zwar ist die Haftung für von Dritten begangenen Urheberrechtsverletzungen („secondary liability") im *Copyright Act* nicht explizit geregelt.[743] Der U.S. Supreme Court hat jedoch klargestellt, dass sowohl das für fast alle Rechtsbereiche geltende Rechtsinstitut der Haftung für fremdes Verschulden als auch die Grundsätze der mittelbaren Haftung im Bereich des *copyright law* anwendbar sind.[744] Seit der Re-

742 *Ott*, GRUR Int. 2008, 564.

743 *Nimmer*, in: Nimmer on Copyright, 2009, § 12.04[A], S. 12-71; *Darrow/Ferrera*, 6 Nw. J. Tech. & Intell. Prop. 1, 7-8 (2007).

744 Vgl. beispielsweise *MGM Studios, Inc. v. Grokster, Ltd.*, 125 S.Ct. 2764, 2776 (2005): *„Although the Copyright Act does not expressly render anyone liable for infringement*

form des *Copyright Act* im Jahre 1976 geht dies in 17 U.S.C. § 106 auch aus dem Gesetzestext hervor: *„ …the owner of a copyright under this title has the exclusive rights to do* and to authorize *any of the following…"* (Hervorhebung durch die Verfasserin). Der Zusatz „and to authorize" wurde vom Gesetzgeber zu dem Zweck eingeführt, um Zweifel an der Geltung der Sekundärhaftung auch für den Bereich des Urheberrechts auszuräumen, indem hierdurch klargestellt wurde, dass nur der Rechtsinhaber berechtigt ist, die Ausübung seiner Rechte Dritten zu überlassen.[745] Daraus folgt im Umkehrschluss, dass eine Rechtsverletzung auch dann vorliegt, wenn ein Nichtberechtigter Dritten die Ausübung dieser Rechte ermöglicht. Wie bereits erwähnt wurde, unterscheidet die urheberrechtliche Sekundärhaftung zwischen zwei Rechtsinstituten, der mittelbaren Rechtsverletzung („contributory infringement") einerseits und der Haftung für fremdes Verschulden („vicarious liability") andererseits.

2. Contributory Infringement

a. Grundlagen des Rechtsinstituts des *contributory infringement*

Das Rechtsinstitut wurde auf Grundlage der allgemeinen Grundsätze des US-amerikanischen Deliktsrechts („tort law") entwickelt.[746] Demnach haftet als *contributory infringer* derjenige, der durch sein Verhalten die unmittelbare Rechtsverletzung fördert oder unterstützt. Als ausreichend wird schon die Bereitstellung von Maschinen oder Werkzeugen angesehen, die der Durchführung der fremden Rechtsverletzung dienlich sind.[747] Die Haftung für *contributory infringement* gründet sich auf das Verhältnis des *contributory infringers* zu der unmittelbar rechtsverletzenden Handlung[748] und erfordert einen eigenen vorwerfbaren Beitrag des *contributory infringers* hierzu. Dies bedeutet, dass der *contributory infringer* für eine Handlung haftet, die er selbst vorgenommen hat und durch die er die

commited by another, … these doctrines of secondary liability emerged from common law principles and are well established in the law… ."; *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 435 (1984); s.a. *Ginsburg*, 50 Ariz. L. Rev. 577, 580 (2008).

745 *Goldstein*, Copyright, 2005, § 6.0, 6:1; dies wird weiterhin auch durch den Wortlaut der Regelung gemäß 17 U.S.C. § 1201(c)(2) belegt, die als Teil des DMCA in den *Copyright Act* aufgenommen wurde und ausdrücklich klarstellt, dass die Haftung für Urheberrechtsverletzungen gemäß den allgemeinen Grundsätzen über *vicarious liability* und *contributory infringement* von den in § 1201 enthaltenen Regelungen unberührt bleibt.

746 *Fonovisa, Inc. v. Cherry Auction, Inc.,* 76 F.3 d 259, 264 (9th Cir. 1996); *Demetriades v. Kaufmann*, 690 F. Supp. 289, 292 (S.D.N.Y. 1971); *Nimmer*, in: Nimmer on Copyright, 2009, § 12.04[A][3], 12-84; *Darrow/Ferrera*, 6 Nw. J. Tech. & Intell. Prop. 1, 8.

747 *Goldstein*, Copyright, 2005, § 6.1, 6:6; *Nimmer*, in: Nimmer on Copyright, 2009, § 12.04[A][3], 12-84.

748 *Goldstein*, Copyright, 2005, § 6.0, 6:4-1.

Rechtsverletzung eines Dritten unterstützt.[749] Im US-amerikanischen Urheberrecht wurde das Rechtsinstitut zum ersten Mal im Jahre 1971 durch den Second Circuit angewendet, der in *Gershwin Publishing v. Columbia Artists Management, Inc.*[750] die Standardformel für *contributory infringement* prägte: *„[o]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a ‚contributory' infringer."*[751]

b. Tatbestandsvoraussetzungen

Voraussetzung der Haftung für *contributory infringement* ist ein wesentlicher Beitrag zu der unmittelbaren Verletzungshandlung.[752] Darüber hinaus muss der *contributory infringer* bestimmte subjektive Anforderungen erfüllen.

aa. Material Contribution

Die Voraussetzung der *material contribution* ist beispielsweise dann erfüllt, wenn die Unterstützungshandlung des *contributory infringers* die unmittelbare Rechtsverletzung erst ermöglicht, d.h. diese ohne den Beitrag des *contributory infringers* nicht hätte stattfinden können.[753] Dasselbe gilt, wenn es dem *contributory infringer* ohne Aufwand möglich gewesen wäre, die rechtswidrige Handlung des unmittelbaren Rechtsverletzers zu unterbinden, er die Urheberrechtsverletzung aber dennoch hat geschehen lassen.[754]

Hinsichtlich des Beitrags des *contributory infringers* zu der unmittelbaren Rechtsverletzung werden – entsprechend der Herkunft des Rechtsinstituts aus dem *tort law* – zwei Ausprägungen unterschieden. Zum einen kann die *material contribution* darin liegen, dass der *contributory infringer* durch eine eigene Handlung zu der unmittelbaren Rechtsverletzung selbst beiträgt.[755] Zum anderen kann die Verbindung zu der unmittelbaren Rechtsverletzung auch in der Zurverfügungstellung von Ausrüstung oder Werkzeugen bestehen, deren Verwendung notwendige Voraussetzung für die Begehung der Rechtsverletzung ist.[756]

749 *Perfect 10 v. Amazon.com*, 487 F.3 d 701 (9th Cir. 2007).
750 *Gershwin Publishing v. Columbia Artists Management, Inc.*, 443 F.2 d 1159 (2 d Cir. 1971).
751 443 F.2 d 1159, 1162.
752 *Nimmer*, in: Nimmer on Copyright, 2009, § 12.04[A][3], 12-85 (2007); *Reese*, 34 Sw. U. L. Rev. 287, 290 (2004).
753 *Fonovisa v. Cherry Auction*, 76 F.3 d 259, 264 (9th Cir. 1996).
754 *RTC v. Netcom*, 907 F. Supp. 1361, 1374.
755 Sogenannte *„contribution of labor"*, vgl. *Goldstein*, Copyright, 2005, § 6.1, 6:7.
756 *Goldstein*, Copyright, 2005, § 6.1, 6:6-7.

bb. Knowledge Element

Weitere Voraussetzung für die Haftung wegen *contributory infringement* ist die Kenntnis des *contributory infringers* von der unmittelbaren Rechtsverletzung. Kenntnis in diesem Sinne bedeutet entweder positive Kenntnis von der konkreten Rechtsverletzung, oder aber zumindest Kenntnis von Umständen, aufgrund derer das Vorliegen einer Rechtsverletzung dem *contributory infringer* hätte bekannt sein müssen.[757] Grundsätzlich gilt zwar im US-amerikanischen Urheberrecht das Prinzip, dass „Unschuldigkeit" im Sinne von Unabsichtlichkeit in Bezug auf die Begehung einer Urheberrechtsverletzung nicht als Verteidigung gegen die Haftung für die Rechtsverletzung verfängt.[758] Im Rahmen der Haftung für *contributory infringement* kommt jedoch ausnahmsweise der Grundsatz des *innocent infringer* zum Tragen, wonach eine Haftung im Falle einer unabsichtlich begangenen Rechtsverletzung ausscheidet, d.h. seitens des Rechtsverletzers zusätzlich bestimmte subjektive Voraussetzungen vorliegen müssen.

(1) Sony: Einschränkung der Haftung für contributory infringement bei Dual-Purpose-Technologien

Bei der Prüfung der Kenntnisvoraussetzung spielt die Art der *material contribution* des *contributory infringers* zu der unmittelbaren Rechtsverletzung eine maßgebliche Rolle. Denn je näher die Handlung des *contributory infringers* dem unmittelbar rechtsverletzenden Verhalten steht, umso eher gehen die Gerichte davon aus, dass dieser auch von der Rechtsverletzung Kenntnis hatte.[759] Jedoch bereitet den Gerichten die Beurteilung der Haftung große Schwierigkeiten, wenn nur eine mittelbare Verbindung zwischen der Tätigkeit des *contributory infringers* und der Rechtsverletzung besteht, beispielsweise wenn der *contributory infringer* durch die Bereitstellung von für die Begehung der unmittelbaren Rechtsverletzung notwendigen Werkzeugen zu dem rechtswidrigen Erfolg beigetragen hat. In solchen Fällen muss der Nachweis erbracht werden, dass der *contributory infringer* von der unmittelbar rechtswidrigen Handlung positive Kenntnis hatte. Dieser Nachweis ist jedoch zumeist schwierig zu führen,[760] da derjenige, der solche Werkzeuge anbietet

757 Vgl. *A&M Records v. Napster,* 239 F.3 d 1004, 1020 (9th Cir. 2001): *"Contributory liability requires that the secondary infringer "know or have reason to know" of direct infringement"*; *RTC v. Netcom,* 907 F. Supp. 1361, 1373-74; *Cable Home Communication Corp. v. Network Prods., Inc.,* 902 F.2 d 829, 845 (11th Circ. 1990).

758 *Goldstein*, Copyright, 2005, § 9.4, 9:16 ff.; vgl. *Lawrence v. Dana*, 15 F. Cas. 26, 60 (C.C.D. Mass. 1869); *Buck v. Jewell-La Salle Realty Co.*, 283 U.S. 191, 198 (1931).

759 *Goldstein*, Copyright, 2005, § 6.1, 6:6.

760 *Goldstein*, Copyright, 2005, § 6.1, 6:11; *Nimmer*, in: Nimmer on Copyright, 2009, § 12.04[A][3][b], 12-87.

und vertreibt, in der Regel keine Kenntnis von der konkreten Verwendung hat, der das Werkzeug durch den Nutzer nach dessen Erwerb zugeführt wird, noch die tatsächliche Verwendung des Werkzeugs beeinflussen kann, wenn dieses seinen Einflussbereich einmal verlassen hat.[761]

Insoweit entschied der Supreme Court Mitte der 80'er Jahre in *Sony Corp. v. Universal City Studios, Inc.*[762] („Sony"), dass zur Erfüllung der subjektiven Voraussetzungen für *contributory infringement* im Zusammenhang mit sogenannten „dual purpose" Technologien („Dual-Purpose-Technologien")[763] nicht ausreicht, dass deren Anbietern bewusst ist, dass diese Technologien auch rechtswidrigen Zwecken dienen können und von einigen Nutzern auch tatsächlich zu solchen Zwecken verwendet werden. Zu diesem Ergebnis kam das Gericht unter Heranziehung eines dem US-amerikanischen Patentrecht entlehnten Grundsatzes.[764] Demnach haftet ein Anbieter von Massenware grundsätzlich nicht für die rechtswidrigen Handlungen seiner Käufer als *contributory infringer*, sofern das jeweilige Produkt auch zur Verwendung für „wesentliche rechtmäßige Zwecke" („substantial noninfringing uses") geeignet ist (sogenannte „staple article of commerce doctrine", nachfolgend „Sony-Doktrin").[765] Nach dem Supreme Court reicht insoweit bereits aus, dass das Produkt zu wesentlichen rechtmäßigen Verwendungen *fähig* ist.[766] Dies bedeutet im Ergebnis, dass die Haftung für *contributory infringement* nicht allein auf den Umstand der Dualität der Nutzungsmöglichkeiten einer Technologie gestützt werden darf. Vielmehr steht die Tatsache, dass die Technologie auch rechtmäßigen Zwecken dienen kann, der Haftung für *contributory infringement* regelmäßig entgegen.[767] Dahinter steht die Erwägung, dass die Rechtsinhaber nicht ohne weiteres in die Lage versetzt werden sollen, auf den Vertrieb einer Massenware allein aufgrund des Umstandes Einfluss zu nehmen, dass diese theoretisch auch zur Verletzung ihrer (Patent- bzw. Urheber-) Rechte verwendet werden kann.[768]

761 *Ginsburg*, 50 Ariz. L. Rev. 577, 581 (2008).
762 *Sony Corp. of America, Inc. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).
763 Hierunter versteht man Technologien, die sowohl zu rechtmäßigen als auch rechtswidrigen Zwecken verwendet werden können, vgl. beispielsweise *Ginsburg*, 50 Ariz. L. Rev. 577, 578 (2008).
764 Vgl. 35 U.S.C. § 271(c).
765 *Goldstein*, Copyright, 2005, § 6.1, 6:12.
766 464 U.S. 417, 442 (1984).
767 464 U.S. 417, 441: *"Unless a commodity has not use except through practice of the patented method, … the patentee has no right to claim that its distribution constitutes contributory infringement."*
768 464 U.S. 417, 440-41: *„When a charge of contributory infringement is predicated entirely on the sale of an article of commerce that is used by the purchaser to infringe a patent, the*

(2) Fortentwicklung der Sony-Doktrin in Napster und Grokster im Kontext des Internets

Die Entscheidung des Supreme Court in *Sony* beeinflusste maßgeblich die Rechtsprechung in Bezug auf die Haftung von ISPs für Urheberrechtsverletzungen, die die Nutzer im Rahmen der von ihnen angebotenen Internetdienste begehen. So griff auch der Ninth Circuit in *Napster*[769] auf die in *Sony* artikulierten Grundsätze zurück. Dementsprechend unterschied er bei der Prüfung der Haftung des Beklagten wegen *contributory infringement* zwischen der objektiven Beschaffenheit des von diesem angebotenen Netzwerks einerseits und dem Verhalten des Beklagten in Bezug auf die operativen Fähigkeiten dieses Netzwerks andererseits.[770] Unter Bezugnahme auf die Sony-Doktrin lehnte das Gericht eine Haftung des Beklagten für *contributory infringement* allein aufgrund der objektiven Beschaffenheit, der „architecture", des Internetdienstes des Beklagten ab:

> „[A]bsent any specific information which identifies infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material. ... To enjoin simply because a computer network allows for infringing use would, in our opinion, violate Sony and potentially restrict activity unrelated to infringing use."[771]

Allerdings fand das Gericht im sonstigen Verhalten des Beklagten genug Anhaltspunkte dafür, dass der Beklagte positive Kenntnis von konkreten rechtswidrigen Inhalten innerhalb seines Internetdienstes hatte. Da der Beklagte weiterhin über die Möglichkeit verfügte, den Zugang zu solchen rechtswidrigen Inhalten zu sperren, bejahte das Gericht dessen Haftung.[772] Damit schloss der Ninth Circuit die Anwendbarkeit der Sony-Doktrin für solche Fälle aus, in denen der Anbieter konkrete Kenntnis von der Rechtsverletzung hat, die er nach der Beschaffenheit seines Systems oder Netzwerk beherrschen kann.[773] In einem solchen Fall hilft der Umstand,

public interest in access to that article of commerce is necessarily implicated. A finding of contributory infringement does not, of course, remove the article from the market altogether; it does, however, give the patentee effective control over the sale of the item. Indeed, a finding of contributory infringement is normally the functional equivalent of holding that the disputed article is within the monopoly granted to the patentee."

769 Vgl. 3. Kapitel, Teil B.II.1.a.

770 *A&M Records v. Napster*, 239 F.3 d 1004, 1020 (9th Cir. 2001).

771 239 F.3 d 1004, 1021 (9th Cir. 2001).

772 239 F.3 d 1004, 1020: *„We nevertheless conclude that sufficient knowledge exists to impose contributory liability when linked to demonstrated infringing use of the Napster system. ... The record supports the district court's finding that Napster has actual knowledge that specific infringing material is available using its system, that it could block access to the system by suppliers of the infringing material, and that it failed to remove that material."*

773 239 F.3 d 1004, 1020-22.

dass die Technologie auch zu *substantial non-infringing uses* verwendet werden kann, dem Anbieter somit nicht, um sich vor einer Haftung als *contributory infringer* zu schützen.[774]

In *Grokster* stellte der Ninth Circuit weiterhin klar, dass seiner Auffassung nach bei Dual-Purpose-Technologien die Haftung für *contributory infringement* des Anbieters aufgrund der Sony-Doktrin grundsätzlich ausscheidet, außer in den wie in *Napster* gelagerten Fällen, d.h. wenn der Anbieter positive Kenntnis von einer konkreten rechtswidrigen Nutzung zu einem Zeitpunkt hat, zu dem er auf dieses rechtswidrige Verhalten reagieren und es hätte verhindern können. Dies gelte sogar dann, wenn andere Anhaltspunkte vorlägen, die auf einen auf die zielgerichtete Förderung der rechtwidrigen Nutzungsmöglichkeiten gerichteten Vorsatz hindeuten.[775] Gegen eine derartige Ausdehnung der Sony-Doktrin wandte sich jedoch in der Berufungsinstanz der Supreme Court[776] und stellte klar, dass hierdurch lediglich ausgeschlossen wird, allein aufgrund der Charakteristika oder der theoretischen Verwendungsmöglichkeiten eines Produkts auf eine vorwerfbare Gesinnung und damit das Vorliegen der subjektiven Voraussetzung der Haftung für *contributory infringement* zu schließen. Darüber hinaus verhindert die Sony-Doktrin jedoch nicht die Berücksichtigung anderer Umstände, die auf einen die Beförderung von rechtswidrigem Verhalten gerichteten Vorsatz („culpable intent") hinweisen und deswegen nach den tradierten Grundsätzen der Sekundärhaftung eine Haftung begründen:

> „Sony's rule limits imputing culpable intent as a matter of law from the characteristics or uses of a distributed product. But nothing in Sony requires courts to ignore evidence of intent if there is such evidence, and the case was never meant to foreclose rules of fault-based liability derived from the common law."[777]

Wenn somit aus anderen Umständen als der bloßen Tatsache, dass die Technologie theoretisch zu Rechtsverletzungen eingesetzt werden kann, ein unmittelbarer, auf die Förderung oder Veranlassung von Rechtsverletzungen gerichteter Vorsatz hervorgeht, bleibt eine Haftung – entgegen der vom Ninth Circuit geäußerten Ansicht – wegen *contributory infringement* auch ohne den Nachweis positiver Kenntnis von konkreten Urheberrechtsverletzungen möglich.[778]

774 *Ginsburg*, 50 Ariz. L. Rev. 577, 582 (2008).
775 *MGM Studios, Inc. v. Grokster Ltd.*, 380 F.3 d 1154, 1162 (9th Cir. 2004).
776 *MGM Studios, Inc. v. Grokster Ltd.*, 125 S. Ct. 2764 (2005); *Ginsburg*, 50 Ariz. L. Rev. 577, 583 (2008).
777 125 S. Ct. 2764, 2779.
778 *Ginsburg*, 50 Ariz. L. Rev. 577, 583 (2008).

(3) Grokster: Einführung der Inducement Rule

In *Grokster*[779] stützte der Supreme Court die Haftung der beklagten ISPs erstmalig auf die „inducement rule" (Veranlasserhaftung). Demnach haftet auch derjenige als *contributory infringer*[780] für Urheberrechtsverletzungen Dritter, der eine Technologie mit dem Ziel vertreibt, hierdurch die Verletzung von Urheberrechten zu fördern.[781] Maßgeblich ist die bewusste und zielgerichtete Förderung der Rechtsverletzungen Dritter durch aktive Unterstützungshandlungen. Keine Rolle spielt insoweit, ob der *contributory infringer* konkrete Kenntnis von den Rechtsverletzungen Dritter hatte. Allerdings rechtfertigen nachweisbare aktive Schritte zur Forcierung von Urheberrechtsverletzungen nach diesem Grundsatz eine Haftung auch dann, wenn die Technologie zu *substantial non-infringing uses* im Sinne der Sony-Doktrin einsetzbar ist.[782] Im Rahmen der Beurteilung, ob solche zielgerichteten Förderungshandlungen vorliegen, ist zu berücksichtigen, dass der normale Handelsverkehr sowie die Entwicklung neuer Technologien nicht beeinträchtigt werden dürfen.[783]

Da es bisher nur eine einzige Entscheidung des Supreme Court zur *inducement rule* im Bereich des Urheberrechts gibt, besteht noch wenig Klarheit darüber, was

779 Vgl. 3. Kapitel, Teil B.II.1.c.

780 Es ist bisher nicht vollständig geklärt, ob die *inducement rule* als eine selbständige Kategorie im Rahmen der Sekundärhaftung für Urheberrechtsverletzungen anzusehen ist, oder als ein Unterfall des *contributory infringement* (so. beispielsweise der Ninth Circuit in *Perfect 10 v. Visa International Service Association*, 494 F.3 d 788, 796 (9th Circ. 2007)). Aus der Entscheidung des Supreme Court geht dies nicht eindeutig hervor, denn das Gericht bezeichnete darin die *inducement rule* generell als eine Ausprägung der „fault-based liability". Einen Hinweis auf die systematische Einordnung der *inducement rule* ergibt sich jedoch daraus, dass der Supreme Court die *inducement rule* im Zusammenhang mit der Sony-Doktrin prüfte, die im Falle ihres Eingreifens das Vorliegen einer Haftung für *contributory infringement* ausschließt. Zudem hatte der Supreme Court dem Ninth Circuit bezüglich der Auslegung der Sony-Doktrin vorgeworfen, dass er diese zu weit ausgelegt hatte, indem er dadurch nicht nur eine Haftung für vermutetes Verschulden („liability resting on imputed intent"), sondern auch aus jedem anderen Grund („liability on any theory") für ausgeschlossen hielt. Dies deutet jedoch darauf hin, dass ein Sachverhalt, der unter die *inducement rule* subsumiert werden kann, die subjektiven Anforderungen der mittelbaren Haftung unabhängig von der Sony-Doktrin erfüllt, d.h. dieser Grundsatz einen Unterfall der mittelbaren Haftung darstellt (vgl. *Nimmer*, in: Nimmer on Copyright, 2009, § 12.04[A][4], 12-109, 12-110, 12-112). *Nimmer* ist jedoch der Auffassung, dass die *inducement rule* als eine separates Institut der Sekundärhaftung anzusehen ist, vgl. *Nimmer*, in: Nimmer on Copyright, 2009, § 12.04[A][4], 12-113, 12-114. Die Einführung der *inducement rule* durch den Supreme Court wird teilweise heftig kritisiert, u.a. als Beispiel für die Überdehnung richterlicher Kompetenzen zu Lasten des Gesetzgebers, vgl. hierzu *Driscoll*, 6 J. Marshall Rev. Intell. Prop. L. 550, 559 (2007).

781 *MGM Studios, Inc. v. Grokster Ltd.*, 545 U.S. 913, 936-37: *„One who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."*

782 125 S. Ct. 2764, 2779.

783 125 S. Ct. 2764, 2780.

unter der maßgeblichen Voraussetzung für die Haftung nach dieser neuen Rechtsregel, nämlich „purposeful, culpable expression and conduct" in Bezug auf die Urheberrechtsverletzung konkret zu verstehen ist.[784] In *Grokster* führten drei Umstände zur Haftung der beklagten ISPs:[785] Nach Auffassung des Gerichts gab es deutliche Hinweise dafür, dass die Beklagten bestrebt waren, sich als die Nachfolger des wegen massenhafter Urheberrechtsverletzungen verurteilten ISP Napster[786] auf dem Markt zu etablieren; Ziel der Beklagten sei es gewesen, die weiterhin ungebrochene Nachfrage nach rechtswidrigen Kopien von urheberrechtlich geschützten Tonaufnahmen der ehemaligen Napster-Nutzer zu bedienen. Weiterhin wurden von den Beklagten keine Filtertechnologien oder andere technische Maßnahmen eingesetzt, um die rechtswidrigen Verwendungsmöglichkeiten der durch die Software der Beklagten errichteten Filesharing-Netzwerke einzudämmen. Schließlich basierte der Umsatz der Beklagten auf Werbeeinnahmen und war damit abhängig von der Anzahl der Nutzer, die die Software der Beklagten nutzten und als Adressaten von Werbebotschaften in Frage kamen.[787]

Aus der Kombination dieser drei Umstände schloss das Gericht, dass die Beklagten ein offensichtliches Interesse daran hatten, ihren Kundenstamm mit allen Mitteln, d.h. auch unter Inkaufnahme und Förderung von Urheberrechtsverletzungen zu vergrößern. Allerdings betonte das Gericht, dass gerade die letzten beiden Gründe, d.h. der Nichteinsatz von Filtertechnologien sowie das werbebasierte Geschäftsmodell der Beklagten, jeweils für sich genommen nicht dafür ausreichen könnten, die Haftung der Beklagten nach der *inducement rule* zu begründen. Denn ansonsten bestehe die Gefahr, die Sony-Doktrin zu unterlaufen, d.h. einen Anbieter lediglich aufgrund der objektiven Beschaffenheit seiner Technologie haftbar zu machen.[788] Andererseits verlangte das Gericht auch nicht ausdrücklich, dass in jedem Falle alle drei Faktoren kumulativ vorliegen müssen, damit eine Haftung nach der *inducement rule* bejaht werden kann.[789]

784 Darrow/Ferrera, S. 11.
785 125 S. Ct. 2764, 2781-2782.
786 Vgl. 3. Kapitel, Teil B.II.1.c.
787 Zur Funktionsweise werbebasierter Geschäftsmodelle vgl. 7. Kapitel, Teil A.III.2.d.
788 545 U.S. 913, 939 (2005): *„... evidence of unlawful objective is given added significance by MGM's showing that neiter company attempted to develop filtering tools or other mechanisms to diminish the infringing activity using their software. ... Of course, in the absence of other evidence of intent, a court would be unable to find contributory infringement liability merely based on a failure to take affirmative steps to prevent infringement, if the device otherwise was capable of substantial noninfringing uses. Such a holding would tread to close to the Sony safe harbor."*
789 *Ginsburg*, 50 Ariz. L. Rev. 577, 586 (2008).

(4) Perfect 10 v. Amazon.com: Fortentwicklung der Voraussetzungen der Haftung von ISPs auf der Grundlage von Sony und Grokster

In *Perfect 10, Inc. v. Amazon.com, Inc*.[790] („Perfect 10 v. Amazon.com") führte der Ninth Circuit die Sony-Doktrin und die *inducement rule* bezogen auf die Haftung von ISPs zusammen. Zunächst stellte das Gericht klar, dass im Rahmen der Haftung für *contributory infringement* zwei Kategorien zu unterscheiden seien: zum einen die aktive Förderung von Rechtsverletzungen durch ein eigenes Verhalten des potenziellen *contributory infringers* und zum anderen der Vertrieb von Dual-Purpose-Technologien, der zur Begehung von Urheberrechtsverletzungen mittelbar beiträgt. Bezüglich letzterer Kategorie scheide die Haftung des ISPs immer dann aus, wenn dessen Technologie auch zu *substantial non-infringing uses* imstande sei.[791] Dessen ungeachtet sei jedoch eine Haftung nach ersterer Kategorie aufgrund der *inducement rule* dann gegeben, wenn ein vorsätzliches Verhalten gerichtet auf die Veranlassung oder Förderung von Rechtsverletzungen vorliege. Auf der Grundlage seiner Rechtsprechung in *Napster* arbeitete der Ninth Circuit sodann die Anforderungen der *inducement rule* für den „context of cyberspace" heraus. Demnach sei die Haftung eines ISPs für *contributory infringement* dann gegeben, wenn dieser positive Kenntnis davon habe, dass bestimmtes rechtswidriges Material in seinem Internetdienst verfügbar ist und er zudem einfache Maßnahmen („simple measures") ergreifen könne, um weiteren Schaden zum Nachteil urheberrechtlich geschützter Werke zu verhindern, den Zugang zu dem rechtswidrigen Material aber dennoch weiterhin gewährt.[792] Damit schränkte der Ninth Circuit den Anwendungsbereich der *inducement rule* im Ergebnis jedoch erheblich ein, da er weiterhin die Kenntnis von konkreten Rechtsverletzungen als Voraussetzung für die Haftung verlangte, obwohl der Supreme Court in *Grokster* ein solches Kenntniserfordernis im Zusammenhang mit der *inducement rule* ausdrücklich nicht erwähnt hatte. Nach dem Supreme Court war vielmehr allein der Nachweis eines „culpable intent" maßgeblich, den das Gericht im Fall der Beklagten unabhängig von deren Kenntnis von konkreten Rechtsverletzungen gegeben sah. In dieser Unabhängigkeit von der positiven Kenntnis liegt der Vorteil der *inducement rule*, was sich daran zeigt, dass die Verurteilung der Beklagten in *Grokster* als *contributory infringer* in den Vorinstanzen gerade daran gescheitert war, dass ihnen aufgrund der dezentralen Struktur des durch ihre Software geschaffenen Netzwerks eine Kenntnis von konkreten Rechtsverletzungen nicht nachgewiesen werden konnte.

790 *Perfect 10, Inc. v. Amazon.com, Inc.*, 487 F.3 d 701 (9th Cir. 2007).
791 487 F.3 d 701, 726 (9th Cir. 2007).
792 487 F.3 d 701, 728-29 (9th Cir. 2007): *„…we hold that a computer system operator can be held contributorily liable if it has actual knowledge that specific infringing material is availible using ist system … and can take simple measures to prevent further damage to copyrighted works, … yet continues to provide access to infringing works."*

(5) Aimster: Gleichsetzung selbst verschuldeter Unkenntnis mit Kenntnis

Noch vor der Entwicklung der *inducement rule* durch den Supreme Court hatte bereits der Seventh Circuit in *Aimster*[793] das Problem des Nachweises der Kenntnis von konkreten Rechtsverletzungen dadurch gelöst, indem er unter bestimmten Voraussetzungen die selbst verschuldete Unkenntnis eines ISPs mit Kenntnis gleichsetzte.

Im konkreten Fall wurde die Haftung des beklagten ISPs als *contributory infringer* damit begründet, dass dieser keine angemessenen Gründe dafür nennen konnte, warum im Rahmen seiner Software eine Verschlüsselungstechnologie eingesetzt wurde, aufgrund derer er den Inhalt der von den Nutzern getauschten Dateien und damit rechtswidriges Verhalten nicht erkennen und einschränken konnte. Nach der vom Gericht in diesem Zusammenhang herangezogenen „cheapest cost avoider"-Theorie wäre insoweit erforderlich gewesen, dass der ISP den Nachweis erbringt, dass ihm wirtschaftlich nicht zumutbar ist, seinen Internetdienst technisch so zu strukturieren, dass dadurch die Begehung von Rechtsverletzungen erschwert bzw. die Beseitigung von erfolgten Rechtsverletzungen erleichtert wird.[794] Aus dem Umstand, dass der Beklagte diese Begründung schuldig blieb, zog das Gericht den Schluss, dass der eigentliche Beweggrund des Beklagten war, sich auf diese Weise wegen mangelnder Kenntnis von Rechtsverletzungen der Haftung für *contributory infringement* zu entziehen.[795] Ein solches vorsätzliches Sichverschließen vor der Kenntnis von Urheberrechtsverletzungen war nach Ansicht des Gerichts jedoch mit Kenntnis gleichzusetzen.[796]

In seiner Entscheidung betonte das Gericht jedoch, dass allein die Tatsache des Einsatzes einer Verschlüsselungstechnologie für die Annahme von *willful blindness* und damit die Haftung des Anbieters für *contributory infringement* nicht ausreichend gewesen wäre.[797] Denn die Verschlüsselung von Daten könne auch dem Schutz der Privatsphäre und damit einem wichtigen Allgemeingut dienen. Eine Haftung komme somit nur in Betracht, wenn diese – wie im Fall des Beklagten von

793 Vgl. 3. Kapitel, Teil B.II.1.b.

794 334 F.3 d 643, 650, 653; *Nimmer*, in: Nimmer on Copyright, 2009, § 12.04[A][3], 12-96. Berichterstatter in diesem Verfahren war Judge Richard A. Posner, der nicht nur Richter an einem der einflussreichen U.S. Courts of Appeals ist, sondern darüber hinaus einer der berühmtesten Vertreter der ökonomischen Analyse des Rechts in den Vereinigten Staaten, woraus sich dieser rechtsökonomische Vorstoß des Gerichts erklärt. Zur Theorie des *„cheapest cost avoider"* vgl. *Schäfer/Ott*, Economic Analysis of Law, 2004, S. 179 ff.: *"From an economic perspective, the practical problems of determining responsibility for an injury can be simplified by asking the question 'which party could have avoided the occurrence of injury at the cheapest cost: the tortfeasor, the victim, or a third party? It is this person who should be responsible for paying compensatory damages."*

795 334 F.3 d 643, 653.

796 334 F.3 d 643, 650.

797 334 F.3 d 643, 650.

Aimster – erkennbar nur zu dem Zweck eingesetzt werde, eine Haftung zu umgehen.[798]

c. Übertragung der Grundsätze des *contributory infringement* auf Web 2.0-Dienste

Zu prüfen ist, ob Web 2.0-Dienste nach den Grundsätzen des *contributory infringement* für die Urheberrechtsverletzungen ihrer Nutzer haften und wie sich die Verfügbarkeit von Content-Identification-Technologien hierauf auswirkt.

Am Vorliegen der ersten Haftungsvoraussetzung, d.h. die Leistung eines wesentlichen Beitrags der Web 2.0-Dienste zu den unmittelbaren Rechtsverletzungen, die durch deren Nutzer begangen werden, bestehen – unabhängig vom Einsatz von Content-Identification-Technologien – keine Zweifel. Die *material contribution* besteht in der Zurverfügungstellung der technischen Funktionen des Web 2.0-Dienstes, durch die es den Nutzern erst ermöglicht wird, digitale Kopien von Multimediawerken der Öffentlichkeit im großen Stil zugänglich zu machen. Die Nutzer könnten die Rechtsverletzungen nicht begehen, wenn ihnen die Anbieter der Web 2.0-Dienste nicht die entsprechenden Werkzeuge wie beispielsweise Speicherplatz und die Funktionen zum Abspeichern und zur Vervielfältigung von Inhalten an die Hand geben würden.

Schwierigkeiten bereitet hingegen die Beurteilung des Vorliegens der subjektiven Haftungsvoraussetzung. Denn nur in seltenen Fällen wird es möglich sein, einem ISP, der einen Web 2.0-Dienst betreibt, positive Kenntnis von einer Urheberrechtsverletzung innerhalb seines Dienstes nachzuweisen. Denn wie bereits dargelegt wurde, werden tagtäglich unzählige Mengen neuer Inhalte in diese Dienste eingestellt. Da das Hochladen dieser Inhalte Teil eines automatisierten Prozesses ist, nimmt der ISP bzw. dessen Mitarbeiter von diesen Inhalten jedoch nicht im Einzelnen Kenntnis. Zudem können Web 2.0-Dienste zu vielfältigen Zwecken genutzt werden, d.h. nicht nur dazu, um Rechte an urheberrechtlich geschützten Multimediawerken zu verletzen. Es handelt sich hierbei somit um Dual-Purpose-Technologien im Sinne der Sony-Doktrin, weswegen das Vorliegen der subjektiven Voraussetzung nicht darauf gestützt werden kann, dass den Betreibern von Web 2.0-Diensten regelmäßig bewusst ist, dass die von ihnen zur Verfügung gestellten technischen Funktionen auch zu rechtswidrigen Zwecken missbraucht werden.

Möglicherweise sind jedoch die Voraussetzungen der vom Supreme Court artikulierten *inducement rule* erfüllt, wenn ein Web 2.0-Dienst innerhalb seines Dienstes keine Content-Identification-Technologien zur Verhinderung von Urhe-

798 334 F.3 d 643, 651.

berrechtsverletzungen einsetzt. Insoweit ist problematisch, dass der Supreme Court in *Grokster* ausdrücklich klargestellt hat, dass diese Tatsache für sich genommen zur Begründung einer Haftung nach der *inducement rule* nicht ausreicht. Es müssen darüber hinaus weitere Umstände vorliegen, aus denen der Veranlassungsvorsatz eindeutig hervorgeht. Insoweit ist zu berücksichtigen, dass hinter der Entscheidung eines ISPs, keine Content-Identification-Technologie einzusetzen, in der Regel auch wirtschaftliche Erwägungen stehen. Denn durch die Ausfilterung von urheberrechtswidrigem Material verliert der Web 2.0-Dienste mit hoher Wahrscheinlichkeit diejenigen Nutzer, die gerade an der Nutzung dieser Inhalte interessiert sind. Zudem basieren die meisten Web 2.0-Dienste auf werbefinanzierten Geschäftsmodellen, weswegen ihr Erfolg von der Attraktivität bei den Nutzern abhängig ist. Dies bedeutet jedoch, dass neben der Tatsache des Nichteinsatzes einer Content-Identification-Technologie seitens des Web 2.0-Dienstes regelmäßig auch ein wirtschaftliches Interesse des ISPs an dem möglichst ungehinderten Zugang zu rechtswidrigem Material gegeben sein wird, womit bereits zwei der drei Kriterien vorliegen, die in *Grokster* für die Haftung des Web 2.0-Dienstes ausschlaggegebend waren. Es bedarf somit nur noch des Hinzutretens eines einzigen weiteren Umstandes, wie beispielsweise einer kompromittierenden Äußerung eines Mitarbeiters in einer Email o.ä., die auf die bewusste Tolerierung des ISPs der rechtswidrigen Inhalte um des geschäftlichen Erfolges willen hindeuten, um eine Haftung des Web 2.0-Dienstes nach der *inducement rule* entsprechend der Vorgaben in *Grokster* auszulösen. Dies bedeutet, dass der Umstand, dass ein ISP keine Content-Identification-Technologieim Rahmen seines Internetdienstes einsetzt, zwar für sich genommen noch nicht dazu ausreicht, eine Haftung als *contributory infringer* zu begründen, den ISP aber zumindest rechtlich sehr angreifbar macht.

Auch ist zu erwarten, dass der Umstand, dass ein ISP innerhalb seines Internetdienstes keine Content-Identification-Technologie einsetzt, zunehmend negative Bedeutung beigemessen werden wird, wenn sich deren Implementierung bei Web 2.0-Diensten mehr und mehr – beispielsweise auch als Ergebnis der UGC-Initiative[799] – als branchenüblich durchsetzt. So hat beispielsweise der District Court, an den das Verfahren nach der Entscheidung des Supreme Court in *Grokster* zurückverwiesen wurde, bereits entschieden, dass in dem Nichteinsatz von Filtertechnologien der Verzicht auf „good faith efforts" zur Eindämmung von Urheberrechtsverletzungen im Rahmen des technisch Möglichen zu sehen ist, woraus auf einen Veranlassungsvorsatz des ISPs im Sinne der *inducement rule* geschlossen werden könne:

> „Although StreamCast is not required to prevent all the harm that is facilitated by the technology, it must at least make a good faith attempt to mitigate the

799 Vgl. 8. Kapitel, Teil A.I.

> massive infringement facilitated by its technology... . Even if filtering technology does not work perfectly and contains negative side effects on usability, the fact that a defendant fails to make some effort to mitigate abusive use of its technology may still support an inference of the intent to encourage infringement... .“[800]

In diese Richtung deutet auch die Rechtsprechung des Seventh Circuit in *Aimster*, wonach sich für einen ISP das Risiko erhöht, als *contributory infringer* zu haften, wenn er zur Verfügung stehende technische Möglichkeiten zur Eindämmung von Rechtsverletzungen nicht nutzt und diese Entscheidung nicht durch zwingende wirtschaftliche Gründe rechtfertigen kann.

Hingegen ist die Tatsache, dass ein Web 2.0-Dienst in seinem Internetdienst freiwillig eine Content-Identification-Technologie einsetzt, als ein Indiz dafür zu werten, dass eine vorwerfbare Gesinnung im Sinne der *inducement rule* in Bezug auf Urheberrechtsverletzungen nicht vorliegt.[801] Denn daran zeigt sich, dass sich der ISP proaktiv darum bemüht, Urheberrechte im Umfeld seines Internetdienstes soweit wie technisch möglich zu schützen. Daraus geht zugleich hervor, dass der ISP nicht daran interessiert ist, von dem Vorhandensein von rechtswidrigem Material innerhalb seines Internetdienstes wirtschaftlich zu profitieren. Der Einsatz von Content-Identification-Technologien bietet einem ISP somit in gewissem Maße Schutz vor einer Haftung als *contributory infringer* auf Grundlage der der *inducement rule*.

3. Vicarious Liability

a. Grundlagen des Rechtsinstituts der *vicarious liability*

Das Rechtsinstitut der *vicarious liability* stellt eine Fortentwicklung des US-amerikanischen Haftungsgrundsatzes des sogenannten „respondeat superior“ („respondeat-superior-Prinzip") dar.[802] Hierdurch werden Fälle erfasst, in denen im Innenverhältnis zwischen dem unmittelbaren Rechtsverletzer und dem „vicarious infringer“ kein Abhängigkeitsverhältnis in Form eines Arbeitsverhältnisses o.ä. besteht, das eine Grundvoraussetzung für die Haftung nach dem *respondeat-superior*-Prinzip ist, die Interessenlage jedoch trotz der fehlenden formalen Beziehung

800 MGM Studios, Inc. v. Grokster, 454 F. Supp. 2 d 966, 989 (C.D. Cal. 2006).
801 *Wu*, Sup. Ct. Rev. 229, 247 (2005); *Katyal*, 32 Colum. J.L. & Arts, 401, 409 (2009).
802 Nach dem *respondeat superior*-Prinzip haftet derjenige, der sich im Geschäftsverkehr durch einen anderen vertreten lässt, für die Rechtsverletzungen seines Vertreters. Der klassische Fall ist die Haftung eines Unternehmens für Urheberrechtsverletzungen, die durch seine Angestellten begangen werden. Vgl. *Nimmer*, in: Nimmer on Copyright, 2009, § 12.04[A][1], S. 12-72; *Goldstein*, Copyright, 2005, § 6.2, 6:17.

zwischen dem Dritten und dem *vicarious infringer* vergleichbar ist. [803] Dies ist grundsätzlich dann der Fall, wenn die Haftung des unmittelbaren Verletzers zur effektiven Durchsetzung der Rechte des Rechtsinhabers nicht ausreicht, da dieser nicht greifbar oder illiquide ist. Zudem ist der *vicarious infringer* regelmäßig in einer besseren Position als der Rechtsinhaber, um das rechtswidrige Verhalten ohne unverhältnismäßig hohen Aufwand zu kontrollieren.[804] Maßgeblich für das Rechtsinstitut der *vicarious liability* ist somit die Art der Beziehung des *vicarious infringers* zu dem unmittelbaren Rechtsverletzer:[805] der *vicarious infringer* haftet dafür, dass er Rechtsverletzungen eines Dritten nicht unterbindet, obwohl er aufgrund seiner Beziehung zu ihm über eine entsprechende Einwirkungsmöglichkeit verfügt.[806] Erstmals anerkannt wurde der Haftungsgrundsatz der *vicarious liability* für Urheberrechtsverletzungen im Jahre 1963 durch den Second Circuit in *Shapiro v. Green*.[807]

803 *Nimmer*, in: Nimmer on Copyright, 2009, § 12.04[A][2], S. 12-81.
804 Vgl. *In re: Aimster Copyright Litigation*, 334 F.3 d 643, 654 (7th Cir. 2003).
805 *Goldstein*, Copyright, 2005, § 6.0, 6:4-1.
806 *Perfect 10 v. Amazon.com*, 487 F.3 d 701, 730-31 (9th Circ. 2007).
807 *Shapiro, Bernstein & Co. v. H.L. Green Co.*, 316 F.2 d 304 (2nd Cir. 1963). Gegenstand dieses Verfahrens war eine Klage gegen ein Unternehmen („Beklagter"), das den Betrieb der Musikabteilungen mehrerer seiner Kaufhäuser einem Konzessionär überlassen hatte, der hierüber Raubkopien von urheberrechtlich geschützten Tonaufnahmen der Kläger vertrieb. In den zwischen dem Beklagten und dem Konzessionär geschlossenen Verträgen war geregelt, dass der Beklagte gegenüber dem Konzessionär und dessen Mitarbeitern weisungsbefugt und zudem berechtigt war, unter bestimmten Umständen Angestellte des Konzessionärs nach freiem Ermessen zu entlassen. Als Gegenleistung für die Gewährung der Konzession hatte der Konzessionär dem Beklagten einen Anspruch auf 10-12 Prozent seiner Bruttoeinnahmen eingeräumt. Von dem Verkauf der Raubkopien hatte der Beklagte keine Kenntnis und war an den hierdurch erzielten Erlösen nicht unmittelbar beteiligt. In erster Instanz war die Klage der Rechtsinhaber mit der Begründung abgewiesen worden, dass der Beklagte die Raubkopien nicht selbst verkauft habe und daher für die vom Konzessionär getätigten Verkäufe nicht haftbar gemacht werden könne. In der Berufungsinstanz hob der Second Circuit dieses Urteil auf. Dabei stellte das Gericht zunächst fest, dass grundsätzlich auch geprüft werden müsse, ob eine an einer Rechtsverletzung nicht unmittelbar beteiligte Person für das rechtswidrige Verhalten eines Dritten aufgrund der zwischen ihr und dem unmittelbaren Verletzer bestehenden Geschäftsbeziehung haftbar gemacht werden kann. Denn über die Fälle der Haftung nach dem respondeat-superior-Prinzip hinaus seien Sachverhalte denkbar, in denen trotz mangelnder „master/servant"-Beziehung alle Elemente vorlägen, die ursprünglich zur Entwicklung und Anwendung des respondeat superior-Prinzips geführt hätten. In diesen Konstellationen sei es zum Zweck einer möglichst effektiven Durchsetzung der Ziele des *copyright law* geboten, auch denjenigen, der eine Verletzungshandlung nicht unmittelbar begangen habe, aber von der Ausbeutung von Urheberrechten profitiere, mit einem Haftungsrisiko zu belasten. Voraussetzung hierfür sei, dass der für fremdes Verschulden Haftende zum einen das Recht und die faktische Möglichkeit zur Überwachung des Dritten sowie zum anderen ein offensichtliches und unmittelbares wirtschaftliches Interesse an der Ausbeutung von Urheberrechten habe. Kenntnis von der Verletzung von Urheberrechten durch den Dritten sei hingegen nicht erforderlich.

b. Tatbestandsvoraussetzungen

Haftungsvoraussetzung ist zum einen, dass der *vicarious infringer* über die rechtliche und tatsächliche Möglichkeit verfügt, das rechtsverletzende Verhalten des Dritten zu kontrollieren, und zum anderen, dass seinerseits ein offensichtliches unmittelbares wirtschaftliches Interesse daran besteht, urheberrechtlich geschützte Werke auszubeuten.[808]

aa. Rechtliche und tatsächliche Kontrollmöglichkeit

Die vom Second Circuit in *Shapiro* erstmals angewendeten Grundsätze zur *vicarious liability* wurden in der Folge fortentwickelt[809] und spielen zunehmend eine wichtige Rolle im Internetkontext im Zusammenhang mit der Haftung von ISPs für Urheberrechtsverletzungen der Nutzer ihrer Internetdienste. Dabei stellt sich zunächst die Frage, wie die Voraussetzung der rechtlichen und tatsächlichen Kontrolle im Zusammenhang mit Internetdiensten zu verstehen ist.

(1) Adobe: Maßgeblichkeit der in Bezug auf das rechtsverletzende Verhalten tatsächlich gegebenen Einwirkungsmöglichkeiten

In *Adobe Sys. Inc. v. Canus Prods., Inc.* (nachfolgend „Adobe")[810] wurden die Grundsätze der *vicarious liability* zunächst auf den Veranstalter einer Computermesse übertragen. Das Gericht kam zu dem Ergebnis, dass der beklagte Veranstalter („Beklagter") für die Urheberrechtsverletzungen, die die Messeteilnehmer durch den Verkauf von Raubkopien von Softwareprogrammen begingen, nicht haftete. Denn der Beklagte erfüllte nach Auffassung des Gerichts nicht die Voraussetzung der tatsächlichen Kontrolle über die unmittelbaren Rechtsverletzer. Zwar hatte sich der Veranstalter vertraglich das Recht vorbehalten, störende Teilnehmer von der Messe zu verweisen. Jedoch wurden die Teilnehmer und ihre Stände vom Sicherheitspersonal des Veranstalters nicht spezifisch auf ihr ordnungsgemäßes Verhalten hin kontrolliert. Die Aufgaben des zahlenmäßig geringen

808 *Nimmer*, in: Nimmer on Copyright, 2009, § 12.04[A][2], S. 12-77. Darüber hinaus ist für die Haftung nach diesem Rechtsinstitut anders als im Rahmen der mittelbaren Haftung nicht erforderlich, dass der Haftende Kenntnis von der Rechtswidrigkeit der Handlung des Dritten hat. Das (Nicht-)Vorliegen von Kenntnis seitens des *vicarious infringers* spielt lediglich eine Rolle für die Rechtsmittel, die dem von der Urheberrechtsverletzung betroffenen Rechtsinhaber gegen den *vicarious infringer* zur Verfügung stehen.

809 Vgl. beispielsweise *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3 d 259 (9th Cir. 1996); *Adobe Sys. Inc. v. Canus Prods., Inc.*, 173 F.Supp. 2 d 1044 (C.D.Cal. 2002).

810 *Adobe Sys. Inc. v. Canus Prods., Inc.*, 173 F.Supp. 2 d 1044 (C.D.Cal. 2002).

Sicherheitspersonals beschränkten sich vielmehr darauf, die Eingänge zur Messe zu überwachen sowie innerhalb der Messe generell nach dem Rechten zu sehen. Mit einer derart reduzierten und mit zusätzlichen Aufgaben betrauten Sicherheitsmannschaft war der Veranstalter nach Auffassung des Gerichts faktisch nicht in der Lage, die Vorgänge an den Verkaufsständen unter anderem auf die Einhaltung des Urheberrechts zu kontrollieren.[811] Insoweit fiel auch ins Gewicht, dass auf der gesamten Messe insgesamt nur etwa hundert Raubkopien der Software des Klägers im Umlauf waren, d.h. der Vertrieb von Raubkopien nicht offensichtlich war und nur einen geringen Anteil an dem Gesamtgeschehen der Messe ausmachte.

(2) Perfect 10 v. Cybernet: Möglichkeit der inhaltlichen Einwirkung auf den unmittelbaren Rechtsverletzer als Indiz für eine bestehende Kontrollmöglichkeit

In *Perfect 10, Inc. v. Cybernet Ventures, Inc.*[812] (nachfolgend „Perfect 10 v. Cybernet") ging es weiterhin um die Frage, unter welchen Umständen anzunehmen ist, dass ein ISP die rechtliche und tatsächliche Kontrolle über urheberrechtswidriges Verhalten ausübt, das lediglich in einem mittelbaren Zusammenhang mit der von ihm angebotenen Dienstleistung steht.

Konkret ging es um die Haftung des Anbieters („Beklagter") eines sogenannten „Age Verification Service" („AVS"), über den Internetnutzer Zugang zu sogenanntem „adult content" erhielten, d.h. zu Internetseiten meist pornographischen Inhalts, deren Nutzung ein bestimmtes Mindestalter voraussetzt.[813] Der Kläger stützte seine Klage darauf, dass viele der Internetseiten, mit denen der Beklagte im Rahmen des AVS kooperierte, unberechtigt urheberrechtlich geschützte Fotografien des Klägers zeigten. Da die Nutzer auch zu solchen Internetangeboten nur unter Nutzung des AVS des Beklagten Zugang erhielten, müsse der Beklagte aufgrund der engen Verknüpfung seiner Dienstleistung mit den fraglichen Internetdiensten für die dort begangenen Urheberrechtsverletzungen haften.[814]

811 173 Supp. 2 d 1044, 1054.

812 *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2 d 1146 (C.D.Cal. 2002).

813 213 F. Supp. 2 d 1146, 1157-58. Im Rahmen des vom Beklagten angebotenen AVS musste ein Nutzer, der auf eine den Dienst des Beklagten verwendende Internetseite zugreifen wollte, sich für eines der vom Beklagten angebotenen Servicepakete anmelden. Hierfür musste er unter anderem die Daten einer Kreditkarte angeben, worüber der AVS das erforderliche Mindestalter des Nutzers mit relativ hoher Sicherheit bestätigen konnte. Erst nach der positiven Bestätigung des Alters des Nutzers erhielt dieser vom AVS die Berechtigung, auf die von ihm gewünschte Internetseite zuzugreifen. Nach Angabe des Beklagten wurde dessen AVS von mehr als 300.000 Webseiten genutzt.

814 Angeblich waren auf etwa 900 der mit dem Beklagten zusammenarbeitenden Internetseiten mehr als 10.000 rechtswidrige Kopien der urheberrechtlich geschützten Fotografien des Klägers vorhanden, vgl. 213 F. Supp. 2 d 1146, 1162.

Das Gericht folgte der Rechtsauffassung des Beklagten. Für die Bejahung der Voraussetzung der rechtlichen und tatsächlichen Kontrolle spielte eine wesentliche Rolle, dass der Beklagte ein sogenanntes „Monitoring-Programm" unterhielt. Dabei wurde die Nutzung des AVS des Beklagten an die Einhaltung bestimmter Vorgaben betreffend Inhalt und Erscheinungsbild der Internetangebote der Kooperationspartner geknüpft. So achtete der Beklagte beispielsweise darauf, dass die auf den Internetseiten seiner Kooperationspartner angebotenen Inhalte ausgewogen blieben, d.h. innerhalb der Internetdienste kein Überangebot an Abbildungen bestimmter Personen entstand. Auch hatte der Beklagte seinen Kooperationspartnern verboten, auf ihren Internetseiten Bilder mit Kinderpornographie anzubieten.[815] Da die Einhaltung dieser Vorgaben vom Beklagten auch aktiv durchgesetzt wurde, bejahte das Gericht die faktische Beherrschungsmöglichkeit des Beklagten in Bezug auf die von seinen Kooperationspartnern angebotenen (rechtswidrigen) Inhalte.

(3) Napster: Verpflichtung der ISPs, die ihnen zur Verfügung stehenden Kontrollmöglichkeiten im Rahmen des technisch Möglichen voll auszuschöpfen

Auch in *Napster*[816] spielte die Frage, ob der beklagte ISP über eine rechtliche und tatsächliche Einwirkungsmöglichkeit in Bezug auf das urheberrechtswidrige Verhalten seiner Nutzer verfügte, eine wichtige Rolle. Hier kam bereits das erstinstanzliche Gericht zu dem Ergebnis, dass seitens des Beklagten eine solche Einwirkungsmöglichkeit gegeben war. Begründet wurde dies damit, dass der Beklagte im Laufe des Verfahrens bekannt gegeben hatte, dass er über zunehmend verbesserte Möglichkeiten verfüge, Nutzer, denen ein urheberrechtswidriges Verhalten vorgeworfen wird, von der Nutzung seines Filesharing-Netzwerks auszuschließen. Zwar hatte der Beklagte mit seiner Äußerung beabsichtigt, seinen Anspruch auf den Schutz der Safe-Harbor-Regelung gemäß § 512(c) zu untermauern.[817] Hingegen sah das Gericht darin die Einlassung, dass der Beklagte das Netzwerk effektiv auf Urheberrechtsverletzungen überwachen und dagegen vorgehen konnte.[818]

815 213 F. Supp. 2 d 1146, 1173.
816 Vgl. 3. Kapitel, Teil B.II.1.a.
817 *Nimmer*, in: Nimmer on Copyright, 2009, § 12.04[A][2], S. 12-83 (2007). Demnach ist unter anderem erforderlich ist, dass der ISP eine sogenannte "repeat infringers policy" unterhält, die u.a. vorsehen muss, dass einem Nutzer auch der Zugang zu dem Internetdienst gesperrt werden kann, wenn er durch wiederholte Rechtsverletzungen auffällt, vgl. 8. Kapitel, Teil B.III.4.a.aa.
818 114 F. Supp. 2 d 896, 920-21: *"... Napster, Inc. itself takes pains to inform thecourt of its improved methods of blocking users about whom rights holders complain. ...This is tantamount to an admission that defendant can, and sometimes does, police its service."*.

Im Berufungsverfahren bestätigte der Ninth Circuit diese Rechtsauffassung. Um einer Haftung für *vicarious liability* zu entgehen, müsse ein ISP vorbehaltene Kontrollrechte vollumfänglich ausüben.[819] Diese Pflicht werde lediglich dadurch begrenzt, dass dem ISP eine solche Kontrolle nur in den Grenzen des technisch Machbaren abverlangt werden könne. In *Napster* konnte der Beklagte die über sein Netzwerk zu tauschenden Dateien nur daraufhin überprüfen, ob sie im für den Internetdienst notwendigen (MP3-)Format vorlagen. Hingegen war es technisch nicht möglich festzustellen, ob die in den Dateien verkörperten Inhalte rechtmäßige Kopien einer urheberrechtlich geschützten Tonaufnahme darstellten. Allerdings bestand die Möglichkeit, die automatisch erstellten Indizes der in dem Filesharing-Netzwerk vorhandenen Dateien anhand der Dateinamen auf bestimmte Tonaufnahmen hin zu durchsuchen und darüber Nutzer, die dem Anschein nach Raubkopien zum Tausch anboten, zu identifizieren. Diese Möglichkeit reichte dem Gericht jedoch aus, um das Vorliegen der erforderlichen Kontrollmöglichkeit zu bejahen.[820]

(4) Grokster & Perfect 10 v. Amazon.com: keine Verpflichtung zur technischen Umgestaltung von Internetdiensten zum Zwecke der Verhinderung von Urheberrechtsverletzungen

In *Grokster*[821] argumentierten die Kläger im erstinstanzlichen Verfahren in Bezug auf die Voraussetzung der rechtlichen und tatsächlichen Kontrolle, dass diese gegeben sei, weil der Beklagte schließlich die Funktionsweise der von ihm angebotenen Software so modifizieren könne, dass die Rechtmäßigkeit der Verwendung der Software durch die Nutzer kontrollierbar werde. Dies könne erreicht werden durch den Einsatz von auf Metadaten oder Content-Identification-Technologien basierenden Technologien, die urheberrechtswidriges Material in dem durch die

819 239 F.3 d 1004, 1023.

820 239 F.3 d 1004, 1024: *„As shown by the record, the Napster system does not „read" the content of indexed files, other than to check that they are in the proper MP3 format. Napster, however, has the ability to locate infringing material listed on its search indices, and the right to terminate users' access to the system. The file name indices, therefore, are within the „premises" that Napster has the ability to police. ... We recognize that the files are user-named and may not match copyrighted material exactly (for example, the artist or song could be spelled wrong). For Napster to function effectively, however, file names must reasonably or roughly correspond to the material contained in the files. Otherwise no user could ever locate any desired music. As a practical matter, Napster, its users and the record company plaintiffs have equal access to infringing material by employing Napster's ‚search function'. ... Napster's failure to police the system's premises, combined with a showing that Napster financially benefits from the continuing availability of infringing files on its system, leads to the imposition of vicarious liability."*.

821 Vgl. 3. Kapitel, Teil B.II.1.c.

Software des Beklagten geschaffenen Netzwerk identifizieren und aussortieren könnten.

Dieser Argumentation schloss sich das Gericht nicht an. Für eine Haftung als *vicarious infringer* reiche nicht aus, dass es *theoretisch* möglich sei, dessen Software so zu verändern, dass die Rechtmäßigkeit des Verhaltens der Nutzer kontrollierbar werde. Vielmehr sei allein maßgeblich, dass der Anbieter die Kontrolle bereits unter den gegebenen Umständen faktisch ausüben könne:

> „Plaintiffs note that Defendants' software already includes optional screens for pornographic/obscene file names, and that it could just as easily screen out copyrighted song titles. Likewise, they note that the software searches "meta data" – information beyond the filename contained in the file itself, including artist, title, album, etc. – and that an effective "meta data" screen could likewise be implemented quite easily. Finally, Plaintiffs contend that Defendants could with relative ease employ emerging "digital fingerprinting" technology that would block out a substantial percentage of copyrighted songs. … However … the obligation to "police" arises only where a defendant has the "right and ability" to supervise the infringing conduct ... While the parties dispute what Defendants feasibly could do to alter their software, here, unlike in Napster, there is no admissible evidence before the Court indicating that Defendants have the ability to supervise and control the infringing conduct (all of which occurs after the product has passed to end-users). The doctrine of vicarious liability does not contemplate liability based upon the fact that a product could be made such that it is less susceptible to unlawful use, where no control over the user of the product exists."[822]

Diese Rechtsauffassung wurde in der Berufungsinstanz vom Ninth Circuit bestätigt. Dabei betonte das Gericht, dass zwischen einem ISP, der bereits der Urheberrechtsverletzung überführt worden sei, und einem bisher noch nicht als *copyright infringer* verurteilten ISP unterschieden werden müsse. Nur hinsichtlich ersterem sei es gerechtfertigt, zum Zwecke der Verhinderung weiterer Urheberrechtsverletzungen ihm gegebenenfalls auch eine Verpflichtung aufzuerlegen, die technischen Parameter seines Internetdienstes zu modifizieren:

> „The district court correctly characterized the Copyright Owners' evidence of the right and ability to supervise as little more than a contention that ‚the software itself could be altered to prevent users from sharing copyrighted files.' ... In arguing that this ability constitutes evidence of the right and ability to supervise, the Copyright Owners confuse the right and ability to supervise with the strong duty imposed on entities that have already been determined to be liable for vicarious copyright infringement; such entities have an obligation to

822 *MGM Studios, Inc. v. Grokster Ltd.*, 259 F.Supp. 2 d 1029, 1045 (C.D. Cal. 2003).

exercises their policing powers to the fullest extent, which in Napster's case included implementation of new filtering mechanisms."[823]

In *Perfect 10 v. Amazon.com*[824] betonte der Ninth Circuit nochmals, dass es im Rahmen der *vicarious liability* nicht darauf ankomme, ob ein ISP theoretisch seine eigenen Organisationsabläufe anders strukturieren und auf diese Weise das Auftreten von Urheberrechtsverletzungen Dritter innerhalb seines Dienstes eindämmen könnte. Dieser Umstand sei allein für die Beurteilung relevant, ob der ISP aufgrund eines eigenen vorwerfbaren Verhaltens als *contributory infringer* haftbar gemacht werden könne.[825] Im Zusammenhang mit dem Rechtsinstitut der *vicarious liability* sei hingegen allein maßgeblich, ob der *vicarious infringer* unter den gegebenen Umständen die rechtswidrigen Handlungen des unmittelbaren Rechtsverletzers tatsächlich hätte unterbinden und damit den Eintritt der Rechtsverletzung hätte verhindern können:

„Perfect 10 argues that Google could manage its own operations to avoid indexing websites with infringing content and linking to third-party infringing sites. This is a claim of contributory liability, not vicarious liability. Although the lines between direct infringement, contributory infringement, and vicarious

823 *MGM Studios, Inc. v. Grokster Ltd.*, 380 F.3 d 1154, 1166 (9th Cir. 2004). Hier nimmt der Ninth Circuit auf eine seiner Entscheidungen im *Napster*-Verfahren Bezug. Nachdem der Beklagte vom Ninth Circuit dem Grunde nach für haftbar befunden und der Rechtsstreit zurückverwiesen worden war, wurde der Beklagte durch das erstinstanzliche Gericht verpflichtet, sämtliche Raubkopien von Werken, bezüglich derer der Beklagte auf eine Verletzung der daran bestehenden Urheberrechte durch illegale Kopien von den Klägern hingewiesen worden war, aus dem Netzwerk zu entfernen. Da es allein mit Hilfe der textbasierten Suchfunktion nicht gelang, alle Raubkopien aufzufinden und zu beseitigen, setzte der Beklagte zusätzlich eine Technologie ein, die unabhängig von den Bezeichnungen der Dateien illegale Kopien urheberrechtlich geschützter Werke auffinden sollte. Das Gericht war jedoch mit dem Ergebnis der Bemühungen des Beklagten nicht zufrieden und ordnete schließlich an, dass der Beklagte seinen Dienst solange suspendieren müsse, bis mit Hilfe der neuen Technologie sichergestellt werden könne, dass keine einzige Raupkopie der Werke der Kläger in dem Netzwerk verbleibe. Hiergegen legte der Beklagte Berufung beim Ninth Circuit ein mit der Begründung, dass der Einsatz der Technologie freiwillig gewesen sei, d.h. insoweit keine Verpflichtung bestehen würde, und er zudem in Bezug auf die Beseitigung von Raubkopien nicht zur Erfüllung eines „zero tolerance"-Standards verpflichtet werden könne. Denn diese Anforderungen gingen weit über die bestehenden Fähigkeiten seines Netzwerks hinaus und liefen somit dem vom Ninth Circuit artikulierten Grundsatz zuwider, dass die Kontrollpflicht eines ISPs ihre Grenze in der technischen Beschaffenheit seines Internetdienstes finden müsse. Der Ninth Circuit kam jedoch zu dem Ergebnis, dass das Gericht lediglich von dem ihm zustehenden Ermessensspielraum Gebrauch gemacht habe in Bezug auf die inhaltliche Ausgestaltung der bereits festgestellten Verpflichtung des Beklagten, Raubkopien aus dem Internetdienst zu entfernen. Insoweit habe das Gericht auch den erst nachträglich eingetretenen Umstand berücksichtigen dürfen, dass sich gezeigt hatte, dass der Beklgate die ihm obliegende Verpflichtung durch die ursprünglich auferlegte Maßnahme des Einsatzes eines textbasierten Filters nicht erfüllen konnte, vgl. *A&M Records, Inc. v. Napster Inc.,* 284 F.3 d 1091, 1098 (9th Circ. 2002).

824 Vgl. 8. Kapitel, Teil B.II.2.b.(bb)(4).

825 Vgl. 8. Kapitel, Teil B.II.2.

liability are not clearly drawn, in general, contributory liability is based on the defendant's failure to stop its own actions which facilitate third-party infringement, while vicarious liability is based on the defendant's failure to cause a third party to stop its directly infringing activities."[826]

bb. Unmittelbarer wirtschaftlicher Vorteil

In Bezug auf die Voraussetzung des unmittelbaren wirtschaftlichen Vorteils zeigt das einschlägige *case law* einen Trend hin zu einer sehr großzügigen Auslegung dieses Tatbestandsmerkmals.

(1) Fonovisa: Wirtschaftlicher Vorteil aufgrund der durch das rechtswidrige Verhalten erzeugten "Sogwirkung"

In *Fonovisa, Inc. v. Cherry Auction, Inc.*[827] ("Fonovisa") war der beklagte Veranstalter eines Flohmarkts, auf dem Händler auch rechtswidrige Kopien von Tonaufnahmen verkauften, nicht prozentual an den Umsätzen der Händler beteiligt und waren die von ihm erhobenen Standgebühren eher gering. Das Gericht ließ jedoch zur Bejahung des unmittelbaren wirtschaftlichen Vorteils ausreichen, dass der Beklagte mittels der von ihm erhobenen Eintritts- und Parkgebühren sowie über seine Beteiligung an dem mit dem Verkauf von Essen und Getränken erzielten Umsatz auch von denjenigen Besuchern des Flohmarkts profitierte, die diesen in erster Linie wegen der Möglichkeit des Erwerbs billiger Raubkopien besuchten.[828] Dies begründete das Gericht mit den *dance hall cases*, nach deren Vorbild die Haftung für *vicarious liability* in *Shapiro* gestaltet worden war und bei denen es um die Haftung der Betreiber von Vergnügungsstätten für darin stattfindende Veranstaltungen gegangen war, in deren Rahmen Urheberrechte verletzt wurden.[829] In diesen Fällen war für die Bejahung der Haftung der Betreiber unter dem Aspekt des unmittelbaren wirtschaftlichen Vorteils ausschlaggebend gewesen, dass sich durch die Veranstaltungen die Attraktivität ihrer Vergnügungsstätte für das Publikum erhöht hatte und sie als Folge daraus von einem verstärkten Besucheraufkommen

826 *Perfect 10, Inc. v. Amazon.com, Inc.*, 487 F.3 d 701, 731 (9th Cir. 2007).
827 *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3 d 259 (9th Cir. 1996).
828 76 F.3 d 259, 263.
829 Vgl. *Shapiro, Bernstein & Co. v. H.L. Green Co.*, 316 F.2 d 304, 307-08 (2 d Cir. 1963)): in den sogenannten „dance hall"-Fällen waren die Betreiber von Vergnügungsstätten für Urheberrechtsverletzungen Dritter haftbar gemacht worden, sofern sie diese Stätten überwachen konnten und einen unmittelbaren wirtschaftlichen Vorteil aus dem Besuch der Veranstaltungen, in deren Rahmen Urheberrechte verletzt wurden, durch zahlendes Publikum zogen.

profitierten. Zu einer derartigen Erhöhung der Attraktivität für Besucher – vom Gericht als „draw“ (Sogwirkung) bezeichnet – habe auch das Angebot von Raubkopien auf dem Flohmarkt des Beklagten geführt, weswegen ein offensichtliches und unmittelbares wirtschaftliches Interesse des Beklagten an dem rechtswidrigen Verhalten der Händler und damit die Haftung des Beklagten für *vicarious liability* gegeben sei.[830]

(2) Adobe: Notwendigkeit eines symbiotischen Verhältnisses zwischen der Rechtsverletzung und dem wirtschaftlichen Erfolg des *vicarious infringer*

In *Adobe*[831] befasste sich das Gericht näher mit dem in Fonovisa eingeführten Kriterium der durch die Urheberrechtsverletzung zugunsten des *vicarious infringer* ausgelösten *draw*. Die Entscheidung in *Fonovisa* müsse so verstanden werden, dass durch dieses zusätzliche Erfordernis eine unerwünschte Ausuferung des Haftungsinstituts vermieden werden sollte, indem das rechtswidrige Verhalten des Dritten dem *vicarious infringer* besondere Vorteile bescheren müsse. So habe in *Fonovisa* ein „symbiotisches Verhältnis“ zwischen den wirtschaftlichen Interessen des Vermieters der Verkaufsstände und dem rechtswidrigen Verhalten der Händler bestanden, da der wirtschaftliche Erfolg des Flohmarkts des Vermieters von dem auf dem Markt vorhandenen Angebot an Raubkopien abhängig gewesen sei. Dies zeige, dass für die Bejahung des *draw* im Sinne von *Fonovisa* der wirtschaftliche Erfolg der Unternehmung des *vicarious infringer* mit den rechtswidrigen Handlungen des unmittelbaren Rechtsverletzers auf das Engste verbunden sein müsse.[832]

(3) Ellison v. Robertson: Unerheblichkeit des relativen Gewichts des durch die Rechtsverletzung ausgelösten wirtschaftlichen Vorteils für den *vicarious infringer*

In *Ellison v. Robertson*[833] („Ellison“) setzte sich weiterhin der Ninth Circuit mit der Frage auseinander, welche Größenordnung die aus dem *draw* folgenden wirtschaftlichen Vorteile zugunsten des *vicarious infringer* erreichen müssen. Gegenstand der Entscheidung war die Haftung eines Access-Providers für die Handlungen eines Usenet-Nutzers, der ohne Erlaubnis der betroffenen Rechtsinhaber Ko-

830 76 F.3 d 259, 263-64.
831 Vgl. 8. Kapitel, Teil B.II.3.b(aa)(1).
832 *Adobe Sys. Inc. v. Canus Prods., Inc.*, 173 F.Supp. 2 d 1044, 1051 (C.D. Cal. 2002).
833 *Ellison v. Robertson*, 357 F.3 d 1072 (9th Circ. 2004).

pien von literarischen Werken erstellt und diese in einer Usenet-Newsgroup, die von den Nutzern vorwiegend zum Austausch von Raubkopien genutzt wurde, öffentlich zugänglich gemacht hatte.[834] Von der Usenet-Newsgroup aus wurden die Raubkopien automatisch auf mit dem Usenet verbundene Server kopiert und anschließend an weitere Server übertragen, darunter auch an diejenigen des Beklagten. Auf diese Weise wurden die Raubkopien Nutzern auf der ganzen Welt zugänglich gemacht.

In erster Instanz war die Haftung des Beklagten abgelehnt worden mit der Begründung, dass ihm aus der Vervielfältigung und Weiterversendung der in das Usenet eingestellten Dateien kein direkter wirtschaftlicher Vorteil erwachsen sei. Anders als in *Napster,* wo die Attraktivität des vom Beklagten angebotenen Netzwerks für dessen Kunden fast ausschließlich darin bestanden habe, dass sie Zugang zu Raubkopien erhielten, könnten die von dem Usenet-Nutzer zugänglich gemachten Raubkopien keine bedeutsame Sogwirkung bezüglich der Inanspruchnahme der Dienstleistung des Beklagten erzeugen. Denn der Zugang zu einer einzelnen der insgesamt ca. 43.000 vom Beklagten unterstützten Usenet-Newsgroups mache lediglich einen minimalen Anteil von ca. 0,00000596 Prozent am gesamten Nutzungsvolumens des Dienstes des Beklagten aus.[835]

Im Berufungsverfahren verneinte der Ninth Circuit zwar im Ergebnis auch eine Haftung des Beklagten, verwahrte sich jedoch dagegen, seine Entscheidung in *Fonovisa* so zu verstehen, dass der *draw* oder *direct financial benefit*, der dem *vicarious infringer* aus der unmittelbaren Verletzungshandlung erwachsen muss, einen erheblichem Umfang annehmen müsse.[836] Ein solches Verständnis würde dazu führen, dass sich gerade große Unternehmen der Haftung regelmäßig mit der Argument entziehen könnten, dass eine einzelne Rechtsverletzung für sie keine wirtschaftlich bedeutsame Sogwirkung erzeugen könne.[837] Dementsprechend sei für die Voraussetzung des *direct financial benefit* nicht maßgeblich, ob ein wirtschaftlicher Vorteil bestimmten Ausmaßes eingetreten sei, sondern allein, dass die Rechtsverletzung einen solchen wirtschaftlichen Vorteil zugunsten des *vicarious infringer* kausal hervorgerufen habe.[838]

834 357 F.3 d 1072, 1075.
835 *Ellison v. Robertson*, 189 F. Supp. 2 d 1051, 1062 (C.D. Cal. 2002).
836 357 F.3 d 1072, 1078.
837 357 F.3 d 1072, 1079.
838 357 F.3 d 1072, 1079: *„The essential aspect of the „direct financial benefit" inquiry is whether there is a causal relationship between the infringing activity and any financial benefit a defendant reaps, regardless of how substantial the benefit is in proportion to a defendant's overall profits."*

(4) Napster: Zukünftige Gewinnchancen ausreichend zur Erfüllung der Haftungsvoraussetzungen der *vicarious liability*

Ihre extremste Ausdehnung erfuhr die Haftungsvoraussetzung des *direct financial interest* jedoch in *Napster*. Dort wurde die Haftung des Beklagten als *vicarious infringer* erstinstanzlich bejaht, obwohl dieser aus dem Betrieb des Filesharing-Netzwerks im Zeitpunkt des Verfahrens noch keine wirtschaftlichen Vorteile gezogen hatte. Das Gericht betrachtete es jedoch als ausreichend, dass die Aussicht bestand, dass Einnahmen auf der Basis des großen Kundenstammes des Beklagten zu einem späteren Zeitpunkt in der Zukunft generiert werden könnten.[839] Der Ninth Circuit bestätigte diese Rechtsauffassung.[840] Somit reicht für das Vorliegen eines *direct financial interest* bereits aus, dass ein wirtschaftlicher Vorteil des *vicarious infringer* aus der unmittelbar rechtswidrigen Handlung in Zukunft erwartet werden kann, selbst wenn er bisher noch nicht realisiert worden sein sollte.[841]

c. Übertragung der Grundsätze der *vicarious liability* auf Web 2.0-Dienste

Zu prüfen ist, ob Web 2.0-Dienste als *vicarious infringer* wegen der Urheberrechtsverletzungen ihrer Nutzer haften und ob sich die Verfügbarkeit von Content-Identification-Technologien hierauf auswirkt.

aa. Rechtliche und tatsächliche Kontrolle über das rechtswidrige Verhalten der Nutzer

Zunächst ist erforderlich, dass der Web 2.0-Dienst rechtlich und tatsächlich dazu in der Lage ist, das rechtswidrige Verhalten der Nutzer zu kontrollieren. Das Recht zur Kontrolle ist im Falle der meisten Web 2.0-Dienste unproblematisch. Denn die

839 *A&M Records, Inc. v. Napster Inc.*, 114 F. Supp. 2 d 896, 921 (N.D. Cal. 2000): *„Although Napster, Inc. currently generates no revenue, its internal documents state that it „will drive [sic] revenues directly from increases in userbase." The Napster service attracts more and more users by offering an increasing amount of quality music for free. It hopes to „monetize" its user base through one of serveral generation revenue models noted in the factual findings. This is similar to the type of financial interest the Ninth Circuit found sufficient for vicarious liability in Fonovisa, where the swap meet's revenues flowed directly from customers drawn by the availability of music at bargain basement prices."* Insoweit spielt auch eine Rolle, dass der Wert eines Filesharing-Netzwerks eng von der Anzahl der daran beteiligten *peers* abhängt, vgl. *Krasilovsky/Shemel*, Music Business, 2007, S. 423: *„Metcalfe's law states that the value of a network increases* exponentially *as a function of the number of nodes"* (Hervorhebung durch die Verfasserin).

840 *A&M Records, Inc. v. Napster Inc.* 239 F.3 d 1004, 1023 (9th Cir. 2001).

841 *Nimmer*, in: Nimmer on Copyright, 2009, § 12.04[A][2], S. 12-83.

ISPs behalten sich in den Nutzungsbedingungen, denen die Nutzer vor der Nutzung des Dienstes zustimmen müssen, regelmäßig vor, rechtswidriges Material bzw. Material, das gegen die Nutzungsbedingungen verstößt, zu entfernen sowie darüber hinaus gegebenenfalls die Nutzungsberechtigung des Nutzers zu beenden.[842] Das Hochladen von Material, das gegen die Rechte Dritter verstößt, wird ausdrücklich untersagt. Lädt der Nutzer dennoch urheberrechtswidriges Material auf den Web 2.0-Dienst hoch, verstößt er somit gegen die Nutzungsbedingungen und berechtigt den ISP, das rechtswidrige Material zu entfernen und den Nutzer von der weiteren Nutzung des Dienstes auszuschließen.

Darüber hinaus muss der Web 2.0-Dienst jedoch auch tatsächlich in der Lage sein, das Verhalten der Nutzer seines Internetdienstes zu kontrollieren. Fraglich ist, ob hierfür ausreicht, dass jeder Web 2.0-Dienst in der Regel eine textbasierte Suchfunktion bietet, mit deren Hilfe die in dem Internetdienst vorhandenen Inhalte durchsucht werden können. Unter Berücksichtigung der Entscheidungen in *Adobe* und *Perfect 10 v. Cybernet* erscheint dies zweifelhaft. Demnach müssen dem *vicarious infringer* Überwachungsmöglichkeiten in einem Umfang zur Verfügung stehen, die eine effektive Verhinderung der Begehung von Rechtsverletzungen ermöglichen, d.h. der *vicarious infringer* muß tatsächlich maßgeblich auf das rechtsverletzende Verhalten einwirken können. Aus der Entscheidung des Ninth Circuit in *Perfect 10 v. Amazon.com* geht weiterhin hervor, dass für das Vorliegen der tatsächlichen Kontrollmöglichkeit nicht ausreicht, dass der ISP durch eine Veränderung der Organisationsabläufe innerhalb seines Dienstes Rechtsverletzungen eindämmen könnte. Vielmehr muss er das rechtsverletzende Verhalten selbst aufhalten können. Davon kann jedoch allein aufgrund des Vorhandenseins einer textbasierten Suchfunktion nicht ausgegangen werden. Denn damit ist es praktisch nicht möglich, die jeden Tag in erheblichem Umfang in Web 2.0-Diensten eingestellten Datenmengen und die in diesem Zusammenhang begangenen Rechtsver-

842 Vgl. z.B. die Nutzungsbedingungen von YouTube, abrufbar unter http://www.youtube.com/t/terms (zuletzt abgerufen am 01.07.2010): *„8.1 Als Inhaber eines Nutzerkontos bei YouTube können Sie Videomaterial („Nutzervideos") und textliche Anmerkungen („Nutzerkommentare") (zusammen: „Nutzerübermittlungen") übermitteln. … 9. Inhalt Ihrer Nutzerübermittlungen - … 9.3 Sie erklären sich damit einverstanden, dass Sie keine Nutzerübermittlungen posten oder hochladen werden, die Gegenstand fremder Eigentumsrechte sind (einschließlich Geheimhaltungs- oder Persönlichkeitsrechte), sofern Sie nicht über eine formelle Lizenz oder Erlaubnis des rechtmäßigen Eigentümers verfügen, welche das Posten des betreffenden Materials und die Einräumung einer Lizenz an YouTube gemäß unten stehender Ziffer 10.1 gestattet. … 9.4 YouTube behält sich das Recht vor (soll aber nicht verpflichtet sein) darüber zu entscheiden, ob Nutzerübermittlungen den Anforderungen an Inhalte entsprechen, wie sie in diesen Bestimmungen enthalten sind. YouTube darf jederzeit, ohne vorherige Ankündigung und nach ausschließlich eigenem Ermessen solche Nutzerübermittlungen entfernen, die diese Bestimmungen verletzen und/oder den zum Hochladen von Nutzerinhalten erforderlichen Zugang eines Nutzers sperren. … 13.3 YouTube kann seine rechtliche Vereinbarung mit Ihnen zu jeder Zeit kündigen, sofern: A.Sie gegen irgendeine Vorschrift der Bestimmungen verstoßen haben…".*

letzungen effektiv zu kontrollieren. Dies scheitert nicht nur an der Menge an Material, das auf diese Weise zu durchsuchen wäre, sondern auch daran, dass es allein durch die Eingabe von bestimmten Suchbegriffen nicht möglich ist, alle rechtswidrigen Inhalte zu „erwischen". Auch stellt das Aussortieren von rechtswidrigem Material über eine Suchfunktion keine unmittelbare Kontrolle über das rechtswidrige Verhalten selbst dar, wie dies in *Perfect 10 v. Amazon.com* gefordert wurde, sondern lediglich eine nachträgliche Beseitigung von dessen Folgen.

Weiterhin besteht aufgrund der eindeutigen Stellungnahme des Ninth Circuit in *Napster, Grokster* sowie *Perfect 10 v. Amazon.com* kein Zweifel daran, dass die theoretische Möglichkeit, Content-Identification-Technologien innerhalb eines Web 2.0-Dienstes einzusetzen und dadurch Rechtsverletzungen zu verhindern, nicht dazu ausreicht, eine (abstrakte) Möglichkeit zur tatsächlichen Kontrolle zu konstruieren, von der der ISP lediglich (bewusst) keinen Gebrauch macht. Denn von einem bisher unbescholtenen ISP kann nicht gefordert werden, die technischen Parameter seines Internetdienstes zum Zwecke des besseren Schutzes für Urheberrechte zu verändern. Es kann lediglich verlangt werden, die bereits zur Verfügung stehenden Überwachungsmöglichkeiten vollumfänglich auszuschöpfen. Damit bleibt im Falle eines ISP, der keine Content-Identification-Technologien einsetzt, aber wiederum nur die Nutzung der textbasierten Suchfunktion zur Aufdeckung von Urheberrechtsverletzungen. Somit kann von dem Vorliegen einer tatsächlichen Möglichkeit zur Kontrolle im Falle eines Web 2.0-Dienstes, der keine Content-Identification-Technologie einsetzt, grundsätzlich nicht ausgegangen werden.

Hingegen ist anzunehmen, dass ein Web 2.0-Dienst, der innerhalb seines Dienstes eine Content-Identification-Technologie einsetzt, über das erforderliche Maß an Kontrolle verfügt. Denn mithilfe dieser Technologien ist es in gewissem Umfang möglich, hochgeladenes Material auf dessen Inhalt zu überprüfen und rechtswidrige von rechtmäßigen Inhalten zu unterscheiden. Dieser Prüfungsprozess wird von der Content-Identification-Technologie automatisiert in Bezug auf jeden Hochladevorgang durchgeführt, so dass eine effektive, da weitgehend lückenlose Kontrolle gegeben ist. Zudem werden nicht nur bereits eingetretene Rechtsverletzungen nachträglich beseitigt, wie dies auch beim Aussortieren von urheberrechtswidrigem Material über eine textbasierte Suchfunktion der Fall ist, sondern sind Content-Identification-Technologien in der Lage, „das Übel an der Wurzel zu packen", d.h. die Rechtswidrigkeit eines hochgeladenen Inhalts bereits beim Hochladen durch den Abgleich mit urheberrechtlich geschützten Material in der korrespondierenden Datenbank mit hoher Sicherheit zu erkennen und das Material daraufhin zu blockieren. Damit wird das Eintreten einer Rechtsverletzung von vornherein verhindert. Dies bedeutet, dass über eine Content-Identification-Technologie auf die *infringing acitivity* selbst und nicht nur auf das rechtswidrige Ergebnis eingewirkt

werden kann. Damit sind die Voraussetzungen der tatsächlichen Kontrollmöglichkeit gegeben.

bb. Unmittelbarer wirtschaftlicher Vorteil

Über die rechtliche und tatsächliche Beherrschungsmöglichkeit hinaus muss der Web 2.0-Dienst einen unmittelbaren wirtschaftlichen Vorteil aus der Rechtsverletzung ziehen. Die Analyse der einschlägigen Präzedenzfälle hat gezeigt, dass hierzu ausreicht, wenn das im Dienst des Web 2.0-Dienstes vorhandene rechtswidrige Material bzw. die darin stattfindenden rechtswidrigen Aktivitäten eine „Sogwirkung" auf andere Nutzer entfaltet, die sich aus diesem Grund dafür entscheiden, den Internetdienst zu nutzen. Nicht maßgeblich ist in diesem Zusammenhang, welche relative Bedeutung der kausal durch die Rechtsverletzung verursachte wirtschaftliche Vorteil des ISPs im Verhältnis zu dessen Gesamtumsatz hat, sowie der Umstand, ob diese Vorteile bereits realisiert wurden oder ihr Eintritt erst in Zukunft zu erwarten ist.

Wie bereits dargelegt wurde, finanzieren sich die meisten Web 2.0-Dienste über Werbeeinnahmen. Ihre Attraktivität für Werbepartner hängt maßgeblich von der Popularität des Internetdienstes bei den Nutzern ab.[843] Daher stellt es für einen Web 2.0-Dienst bereits dann einen wirtschaftlichen Vorteil dar, wenn aufgrund des urheberrechtswidrigen Materials, das in diesem Dienst vorhanden ist, neue Nutzer angelockt werden. Denn jeder neue Nutzer erweitert den Kundenstamm des Web 2.0-Dienstes und damit gleichzeitig die Anzahl potentieller Adressaten von Werbebotschaften, wodurch die Attraktivität des Internetdienstes für Werbepartner steigt. Ein kausal durch das rechtswidrige Verhalten der Nutzer verursachter unmittelbarer wirtschaftlicher Vorteil des Web 2.0-Dienstes liegt somit regelmäßig vor.

cc. Zwischenergebnis

Als Ergebnis lässt sich somit festhalten, dass Web 2.0-Dienste, die Content-Identification-Technologien nicht einsetzen, grundsätzlich nicht als *vicarious infringer* haften, da ihnen nach dem einschlägigen *case law* die tatsächliche Möglichkeit zur Kontrolle von Rechtsverletzungen fehlt. Hingegen erfüllen Web 2.0-Dienste, die innerhalb ihrer Dienste Content-Identification-Technologien implementiert haben, aufgrund der Möglichkeiten zur Identifikation und Beseitigung von rechtswidrigem Material, die diese Technologien eröffnen, diese Voraussetzung. Aufgrund

843 Vgl. 7. Kapitel, Teil A.III.d.

des weiten Begriffsverständnisses betreffend die Voraussetzung des unmittelbaren wirtschaftlichen Vorteils ist zudem davon auszugehen, dass Web 2.0-Dienste auch diese Voraussetzung regelmäßig erfüllen, insbesondere wenn sie auf einem werbefinanzierten Geschäftsmodell basieren. Daher ist ihre Haftung als *secondary infringer* in Bezug auf die Urheberrechtsverletzungen ihrer Nutzer grundsätzlich zu bejahen.

4. Ergebnis

Die vorhergehende Analyse der Haftung von Web 2.0-Diensten nach den einschlägigen Rechtsinstituten der Sekundärhaftung des US-amerikanischen Urheberrechts hat gezeigt, dass zum gegenwärtigen Zeitpunkt sowohl der Einsatz von Content-Identification-Technologien als auch der bewusste Verzicht hierauf negative haftungsrechtliche Folgen haben kann.

Zum einen läuft ein ISP, der innerhalb seines Web 2.0-Dienstes freiwillig eine Content-Identification-Technologie einsetzt, Gefahr, aus diesem Grund als *vicarious infringer* in Bezug auf die von Nutzern begangenen Rechtsverletzungen haftbar gemacht zu werden. Denn aufgrund der durch eine solche Technologie eröffneten Möglichkeit der Verhinderung des unerlaubten Hochladens von Kopien urheberrechtlich geschützter Multimediawerke ist seitens des ISPs die Möglichkeit der tatsächlichen Kontrolle über das rechtswidrige Verhalten seiner Nutzer gegeben. Da im Falle eines werbefinanzierten Web 2.0-Dienstes zudem regelmäßig das Erfordernis eines aus der Rechtsverletzung resultierenden unmittelbaren wirtschaftlichen Vorteils zu bejahen ist, erfüllt ein ISP, der eine Content-Identification-Technologie einsetzt, grundsätzlich die Voraussetzungen der *vicarious liability*.

Hingegen sieht sich ein ISP, der auf den Einsatz einer Content-Identification-Technologie innerhalb seines Web 2.0-Dienstes bewusst verzichtet, dem Risiko der Haftung als *contributory infringer* ausgesetzt. Denn aufgrund dieses bewussten Verzichts sowie des dahinterstehenden wirtschaftlichen Interesses an einem ungehinderten Zugang der Nutzer auch zu rechtswidrigem Material sind in dieser Konstellation bereits zwei der drei Umstände gegeben, die in *Grokster* die Haftung der Beklagten nach der vom Supreme Court auf das *copyright law* übertragenen *inducement rule* begründeten. Insoweit bedarf es somit nur noch des Hinzutretens eines einzigen weiteren Umstandes, der als ein Hinweis auf einen *culpable intent* des ISP gewertet werden kann, damit eine Haftung dieses ISPs nach diesem Haftungsgrundsatz gegeben ist. Auch ließe sich die Haftung eines solchen ISPs dadurch begründen, indem man der vom Seventh Circuit in *Aimster* artikulierten Rechtsauffassung folgt, dass ein willentliches Sichverschließen vor der Kenntnis von Rechtsverletzungen der positiven Kenntnis gleichzusetzen ist und in dem Verzicht

auf den Einsatz von Content-Identification-Technologien ein solches willentliches Sichverschließen zu sehen ist, welches dann ebenfalls zu einer Haftung als *contributory infringer* führt.

Als Ergebnis bleibt somit festzuhalten, dass sich der Betreiber eines Web 2.0-Dienstes auf der Ebene der Haftungsbegründung in einem Dilemma befindet. Denn egal wie er sich entscheidet, erwachsen ihm hieraus unter dem Aspekt der urheberrechtlichen Sekundärhaftung negative Folgen.

III. Die Haftungsbeschränkung für Host-Provider gemäß 17 U.S.C. § 512(c)

1. Einführung

Mit dem II. Titel des DMCA, dem „Online Copyright Infringement Liability Limitation Act", wurde 17 U.S.C. § 512 (nachfolgend „§ 512") in den *Copyright Act* eingeführt. Demnach werden ISPs von der Haftung für Urheberrechtsverletzungen befreit, wenn sie bestimmte Anforderungen erfüllen (sogenannter „safe harbor"). Die Regelung ist in vier Tatbestände unterteilt, orientiert an vier unterschiedlichen Arten von Leistungen, die von ISPs im Internet typischerweise erbracht werden:[844]

(1) die durchlaufende (transitorische) Kommunikation von Daten,[845]
(2) die kurzeitige Zwischenspeicherung von Daten,[846]
(3) die längerfristige Speicherung von Daten im Auftrag eines Nutzers,[847] sowie
(4) das Anbieten von Suchmaschinen[848]

(nachfolgend „Safe-Harbor-Regelungen"). Erfüllt ein ISP die Voraussetzungen eines dieser vier Tatbestände, können gegen ihn keine Schadensersatzansprüche wegen der von den Nutzern im Rahmen seines Internetdienstes begangenen Urheberrechtsverletzungen geltend gemacht werden. Weiterhin können nur in sehr engen Grenzen Handlungs- oder Unterlassungsverfügungen („injunctions") gegen ihn ergehen.[849] Die Haftungsbeschränkungen gemäß § 512 werden hinsichtlich ihrer praktischen Auswirkungen, insbesondere im Vergleich mit den ebenfalls durch den

844 *US Copyright Office*, DMCA Summary, 1998, S. 8.
845 Vgl. 17 U.S.C. § 512(a).
846 Sogenanntes „system caching", vgl. 17 U.S.C. § 512(b); unter *system caching* versteht man die Zwischenspeicherung aktueller oder in Bearbeitung befindlicher Dokumente auf schnellen Speichermedien (Festplatte oder Arbeitsspeicher des lokalen Rechners), um zeitaufwendige Zugriffe auf Medien mit längeren Zugriffszeiten zu vermeiden.
847 Vgl. 17 U.S.C. § 512(c).
848 Vgl. 17 U.S.C. § 512(d).
849 Vgl. 17 U.S.C. § 512(j).

DMCA eingeführten Vorschriften über technische Schutzmaßnahmen, überwiegend positiv gewertet.[850] Ihnen sei es zu verdanken, dass das Internet bzw. die hierüber angebotenen Dienstleistungen sich derart rasant hätten fortentwickeln können.[851]

2. Entstehungsgeschichte

> „Title II [DMCA] will provide certainty for copyright owners and internet service providers with respect to copyright infringement liability online."[852]

a. Keine Vorgaben in den WIPO-Internetverträgen zu Haftungsbeschränkungen zugunsten ISPs

§ 512 wurde im Zuge der Umsetzung der WIPO-Internetverträge durch den DMCA in den *Copyright Act* eingefügt. Im Unterschied zu den Regelungen über technische Schutzmaßnahmen des I. Titels des DMCA[853] enthielten die WIPO-Internetverträge[854] jedoch keine Vorgaben hinsichtlich der Beschränkung der Haftung von ISPs für innerhalb ihrer Internetdienste begangene Urheberrechtsverletzungen der Nutzer. Vielmehr war in diesem Zusammenhang ursprünglich geplant, im Rahmen der WIPO-Konferenz in Genf klarzustellen, dass unter dem im RBÜ verwendeten Begriff der Vervielfältigung („reproduction") jede unmittelbare oder mittelbare, dauerhafte oder auch nur vorübergehende Vervielfältigung eines urheberrechtlich geschützten Werkes zu verstehen ist. Dieses Vorhaben scheiterte jedoch am Widerstand der im Internet tätigen Unternehmen, die von einer solchen Klarstellung

850 *Seidenberg*, ABA Journal, February 2009, S. 48; *Holznagel*, GRUR Int 2007, 971, 982; *Pankoke*, Von der Presse- zur Providerhaftung, 2000, S. 174 f.

851 Vgl. beispielsweise *Seidenberg* s.o.; *Kravets*, 10 Years Later, Misunderstood DMCA is the Law That Saved the Web, WIRED, 27.10.2008, http://Weblog.wired.com/27bstroke6/2008/10/ten-years-later.html (zuletzt abgerufen am 01.07.2010); *Heise Online*, Zehn Jahre Digital Millennium Copyright Act: Recht fürs Internet?, 28.10.2008, http://www.heise.de/newsticker/meldung/118043 (zuletzt abgerufen am 01.07.2010); *Timmer*, A decade of the DMCA: keep the Safe Harbor, ditch the rest, Ars Technica, 28.10.2008, http://arstechnica.com/news.ars/post/20081028-adecade-of-the-dmca-keep-the-safe-harbor-ditch-the-rest.html (zuletzt abgerufen am 01.07.2010).

852 Sen. Rep. 105-190, S. 2.

853 Vgl. 4. Kapitel, Teil D.II.1.

854 Vgl. 4. Kapitel, Teil D.I.

erhebliche Haftungsnachteile erwarteten.[855] So forderte beispielsweise die „Digital Future Alliance", ein Zusammenschluss US-amerikanischer Unternehmen auf Seiten der Rechtsinhaber, von dieser Klarstellung Abstand zu nehmen, da sie im Ergebnis ein neues digitales Nutzungsrecht zugunsten der Rechtsinhaber schaffen würde. Demgegenüber forderte diese Allianz, für alle Vertragstaaten verbindliche Bestimmungen dahingehend einzuführen, dass ISPs von der Haftung für Urheberrechtsverletzungen der Nutzer im Internetkontext freizustellen sind.[856]

Dazu kam es im Ergebnis nicht. Allerdings erreichten die ISPs mit ihrem Widerstand, dass es betreffend die Reichweite des Vervielfältigungsrechts lediglich zu einem „Agreed Statement" kam. Darin wurde festgehalten, dass das Vervielfältigungsrecht gemäß Art. 9 RBÜ auch im digitalen Kontext uneingeschränkt Geltung entfaltet. Somit stellt auch die Speicherung einer digitalen Kopie eines urheberrechtlich geschützten Werks innerhalb eines elektronischen Mediums eine Vervielfältigungshandlung dar.[857] Mit diesem *Agreed Statement* wurden jedoch keine konkreten Vorgaben zu dessen Durchsetzung auf der Ebene der Rechtssysteme der Vertragsstaaten verbunden. So blieb es im Ergebnis den einzelnen Vertragsstaat überlassen zu entscheiden, welche Folgen sich hieraus auf nationaler Ebene im Hinblick auf die Haftung von ISPs für die Rechtsverletzungen der Nutzer ihrer Internetdienste ergeben sollten.[858]

b. US-amerikanische Bemühungen um eine Regelung der Haftung von ISPs seit der Regierung Clinton

Vor diesem Hintergrund empfahl das Senate Foreign Relations Committee dem US-amerikanischen Gesetzgeber die Ratifizierung der WIPO-Internetverträge unter der Bedingung, dass das Gesetz zur Umsetzung der WIPO-Internetverträge auch

855 Vgl. S. Exec. Rep. 105-25, S. 4 (October 14, 1998): *„The most contentious copyright issue at the WIPO Diplomatic Conference related to a draft article dealing with the reproduction right and its application to digital or electronic formats. Internet service providers, telephone companies, and other telecommunications entities generally objected to application of the reproduction right to indirect or temporary copying by computers transferring files on the Internet and other computer networks. In the end, draft Article 7 on the reproduction right was dropped entirely from the text of the Copyright Treaty."*

856 *von Lewinski/Gaster*, ZUM 1997, 607, 614-615.

857 *„The reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted thereunder, fully apply in the digital environment, in particular to the use of works in digital form. It is understood that the storage of a protected work in digital form in an electronic medium constitutes a reproduction within the meaning of Article 9 of the Berne Convention."*; vgl. hierzu weiterführend *Reinbothe/von Lewinski*, Annex to Article 1(4) WCT, S. 37ff.

858 S. Rep. 105-190, S. 5; *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.01[B][1], S. 12B-21.

eine Regelung betreffend die Haftung von ISPs enthalten müsse.[859] Diesbezüglich hatte es in den USA schon lange vor der WIPO-Konferenz umfangreiche, jedoch ergebnislose Anstrengungen gegeben.

Bereits im Jahr 1993 hatte die US-amerikanische Regierung unter Präsident Bill Clinton die sogenannte „Information Infrastructure Task Force" („IITF") gebildet, die ihrerseits die sogenannte „Working Group on Intellectual Property Rights" („IP Working Group") ins Leben gerufen hatte. Diese wurde mit der Aufgabe betraut, die Auswirkungen der neuen digitalen Technologien auf das Recht des geistigen Eigentums zu untersuchen und Empfehlungen bezüglich etwaiger dadurch notwendig werdender Änderungen in Recht und Politik auszusprechen.[860] Nach Abschluss dieser Untersuchung veröffentlichte die IP Working Group ein „White Paper" mit einem Bericht über die gefundenen Ergebnisse.[861] Auf der Grundlage des White Paper wurde der „National Information Infrastructure Copyright Protection Act of 1995" entworfen. Dessen Verabschiedung scheiterte jedoch an der fehlenden Einigung der betroffenen Interessengruppen.[862] Denn bereits zu diesem Zeitpunkt drängten die ISPs auf die Einführung eines formalisierten Benachrichtigungsverfahrens betreffend Urheberrechtsverletzungen. Im Rahmen dieses Verfahrens hätte es in erster Linie den Rechtsinhabern oblegen, einen ISP über die Existenz von rechtswidrigem Material innerhalb seines Dienstes zu benachrichtigen, und wäre der ISP erst im Anschluss daran zur Beseitigung des Materials verpflichtet gewesen.[863] Dieser Ansatz – der in Form des Notice&Takedown-Verfahrens gemäß § 512(c)(3)[864] wenige Jahre später Gesetz wurde – war von den Rechtsinhabern jedoch abgelehnt worden, da diese nicht einseitig mit dem Aufwand und den Kosten

859 S. Exec. Rep. 105-25, S. 17: *„This need for such clarification was anticipated during the Diplomatic Conference that adopted the WIPO Treaties. The Conference adopted an "agreed statement" regarding Article 8 of the WIPO Copyright Treaty, which states that Internet service providers (ISPs) should not be held liable when they merely provide "physical facilities for enabling or making a communication." In order to address this issue, the WIPO Treaties implementing legislation (H.R. 2281) has embodied within it a compromise regarding the issue of copyright infringement liability for ISPs."* Dementsprechend lautete es im Beschluß des Senats hinsichtlich der Ratifizierung und Umsetzung der WIPO-Verträge: *„Provisos. – The advice and consent of the Senate is subject to the following provisos: (1) Condition for Ratification. – The United States shall not deposit the instruments of ratification for these Treaties until such time as the President signs into law a bill that implements the Treaties, and that includes clarifications to United States law regarding infringement liability for on-line service providers, such as contained in H.R. 2281."*; s. a. S. Rep. 105-190, S. 19.

860 S. Rep. 105-190, S. 2.

861 *IITF*, Intellectual Property and the National Information Infrastructure, 1995. Zudem hielt die Working Group eine Konferenz bezüglich der sich aus der zunehmenden Digitalisierung ergebenden Probleme im Zusammenhang mit der Fair-Use-Doktrin ab (Conference on Fair Use, nachfolgend „CONFU") und veröffentlichte darüber ebenfalls einen Bericht.

862 S. Rep. 105-190, S. 4.

863 *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.01[B][2], 12B-22.

864 Vgl. 8. Kapitel, Teil B.III.4.f.

des *copyright policing* belastet werden wollten.[865] Sie argumentierten zudem, dass die von den ISPs vorgeschlagene Benachrichtigungspflicht gegen das in Art. 5 Abs. 2 RBÜ enthaltene Verbot verstoßen würde, urheberrechtlichen Schutz von formalen Anforderungen abhängig zu machen. Damit gelang es den Rechtsinhabern zum damaligen Zeitpunkt noch, den Gesetzgeber zum Verzicht auf eine solche Regelung zu bewegen.[866] Auch war im White Paper von Haftungsbeschränkungen für ISPs grundsätzlich abgeraten und empfohlen worden, diese weiterhin ebenso wie andere im offline-Vertrieb von Multimediawerken tätige Intermediäre zu behandeln, d.h. unterschiedslos nach den allgemeinen Grundsätzen des US-amerikanischen Urheberrechts haften zu lassen.[867] Denn nach Auffassung der IP Working Group war zu befürchten, dass durch die Einführung von Haftungsbeschränkungen die Anreize zur Entwicklung von Mechanismen zur Minimierung der Haftungsrisiken von ISPs einerseits und zur Verbesserung des Schutzes der urheberrechtlichen Positionen der Rechtsinhaber andererseits verloren gehen würden.[868] Weiterhin galt es nach Ansicht der die *IP Working Group* eine faktische Rechtlosstellung der Rechtsinhaber zu vermeiden, wenn beispielsweise aus bestimmten Gründen der Zugriff auf den unmittelbaren Rechtsverletzer scheitert.

Im Rahmen des Gesetzgebungsverfahrens zum DMCA gelangten Rechtsinhaber und ISPs nach dreimonatigen intensiven Verhandlungen dann aber doch noch zu einer Einigung in der Frage der Haftung von ISPs.[869] Der den Parteien mühsam abgerungene Kompromiss basierte auf zwei grundsätzlichen Erwägungen.[870] Zum einen wollte man den Rechtsinhabern ausreichende Anreize bieten, damit diese

865 *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.01[B][2], 12B-22.

866 Daraus erklärt sich, warum der Gesetzgeber bei Einführung von § 512(c)(3) betonte, dass durch die Einführung des Notice&Takedown-Verfahrens die Takedown-Notice nicht zu einer materiellen Voraussetzung der Durchsetzbarkeit der Rechte der Rechtsinhaber werde, da ISPs bei Kenntnis von einer Rechtsverletzung auch ohne das Vorliegen einer solchen Benachrichtigung zur Entfernung des rechtswidrigen Materials verpflichtet seien. Die Takedown-Notice erleichtere den Rechtsinhabern lediglich den Nachweis der Kenntnis eines ISPs von einem Rechtsverstoß. Vgl. S. Rep. 105-190, S. 54.

867 *IITF*, Intellectual Property and the National Information Infrastructure, 1995, S. 122-124; *Dimitrieva*, 16 Santa Clara Computer & High Tech. L.J. 233, 244-45 (2000).

868 Unter diesen sogenannten „marketplace tools" verstand die Working Group beispielsweise Versicherungsschutz für Internetanbieter gegen ihnen aus Rechtsverletzungen der Nutzer resultierende Schäden (beispielsweise in Form von auf Schadensersatz gerichteten Urheberrechtsklagen), die Verschiebung des Haftungsrisikos von den Internetdiensten auf die Nutzer durch Abschluss von Verträgen mit entsprechenden Garantie- und Freistellungsklauseln, die Aufklärung der Nutzer über Urheberrechtsverletzungen sowie der Einsatz von technischen Schutzvorrichtungen.

869 S. Rep. 105-190, S. 7, 9.

870 S. Rep. 105-190, S. 8: *„Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy. Legislation implementing the treaties provides this protection and creates the legal platform for launching the global digital on-line marketplace for*

ihre urheberrechtlich geschützten Multimediawerke auch im Internet verfügbar machen würden. Unter diesem Aspekt hielt man es für unentbehrlich, angesichts der Leichtigkeit, mit der im digitalen Zeitalter Kopien von Multimediawerken hergestellt und verbreitet werden können, einen möglichst effektiven Schutz vor Urheberrechtsverletzungen im digitalen Umfeld zu gewähren. Zum anderen wollte man die Fortentwicklung des Internets und der damit neu eröffneten Vertriebs- und Vermarktungsmöglichkeiten sicherstellen. Diesen Fortschritt sah man jedoch gefährdet, wenn die ISPs als der „Motor" dieser Weiterentwicklung keine Klarheit über den Umfang ihrer Haftung für Rechtsverletzungen Dritter erhalten würden. Diese beiden, teilweise im Widerspruch zueinander stehenden Interessen sollten nunmehr durch das neue Gesetz in Einklang gebracht werden.[871]

3. Grundlagen der Safe-Harbor-Regelungen gemäß § 512

a. Systematik

Ausgangspunkt für die Schaffung der Haftungsbeschränkung gemäß § 512 waren die Kernaussagen der *Netcom*-Entscheidung.[872] Die entscheidende Weichenstellung dieser Entscheidung bestand darin, ISPs vorwiegend als passive Intermediäre einzuordnen. Aus diesem Grund können ihnen die Handlungen der Nutzer ihrer Internetdienste aus haftungsrechtlicher Sicht grundsätzlich nicht zugerechnet werden, es sei denn, es liegt eine zusätzliche „affirmative action" oder „causation" seitens des ISPs in Bezug auf die konkrete Rechtsverletzung vor.

Der Gesetzgeber beabsichtigte zunächst, diese Kernaussage aus *Netcom* zu kodifizieren. Demnach sollte die unmittelbare Haftung von ISPs im Zusammenhang

> *copyrighted works. It will facilitate making available quickly and conveniently via the Internet the movies, music, software, and literary works that are the fruit of American creative genius. It will also encourage the continued growth of the existing off-line global marketplace for copyrighted works in digital format by setting strong international copyright standards. At the same time, without clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet. In the ordinary course of their operations service providers must engage in all kinds of acts that expose them to potential copyright infringement liability. For example, service providers must make innumerable electronic copies by simply transmitting information over the Internet. Certain electronic copies are made to speed up the delivery of information to users. Other electronic copies are made in order to host World Wide Web sites. Many service providers engage in directing users to sites in response to inquiries by users or they volunteer sites that users may find attractive. Some of these sites might contain infringing material. In short, by limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand."*

871 *Goldstein*, Copyright, 2005, § 6.3, 6:24; *Darrow/Ferrera*, 6 Nw. J. Tech. & Intell. Prop. 1, 12 (2007); *Cloak*, 60 Vand. L. Rev. 1559, 1569 (2007).

872 Vgl. 8. Kapitel, Teil B.I.3.b.

mit Urheberrechtsverletzungen, die sich im Zusammenhang mit automatisierten technischen Abläufen innerhalb ihrer Internetdienste zutragen, ausdrücklich ausgeschlossen werden.[873] Weiterhin sollten die Tatbestandsvoraussetzungen der Rechtsinstitute der urheberrechtlichen Sekundärhaftung konkretisiert und an erhöhte Anforderungen geknüpft werden sowie die insoweit den Rechtsinhabern gegen ISPs zur Verfügung stehende Rechtsmittel beschränkt werden. Von diesem Ansatz kam der Gesetzgeber jedoch im Laufe des Gesetzgebungsverfahrens ab. Anstattdessen entschied er sich dazu, nur die Folgen der Haftung von ISPs für Urheberrechtsverletzungen im Zusammenhang mit bestimmten typisierten Tätigkeiten zu beschränken.[874] Die endgültige Fassung des Gesetzes lässt daher die Grundsätze der *primary* und *secondary liability*,[875] die in Bezug auf die Haftung von ISPs für Urheberrechtsverletzungen der Nutzer entwickelt wurden, unberührt.[876] Ihrer Konzeption nach gewähren die Safe-Harbor-Regelungen ISPs somit lediglich ein Mindestmaß an Schutz in Bezug auf die Folgen einer dem Grunde nach gegebenen Haftung für die Urheberrechtsverletzungen der Nutzer, lassen sie die Grundsätze des *common law* über die Haftung für Urheberrechtsverletzungen Dritter ansonsten jedoch unberührt.[877]

Streng genommen kommt die Haftungsbeschränkung daher grundsätzlich erst nach der Feststellung der Haftung eines Internetdienstes gemäß den allgemeingültigen Rechtsgrundsätzen der urheberrechtlichen Primär- und Sekundärhaftung zum Tragen und bestimmt, welche Folgen sich hieraus ergeben.[878] Dementsprechend sind die Safe-Harbor-Regelungen an und für sich erst auf zweiter Stufe, d.h. nach der Prüfung und Feststellung Haftung eines ISPs als *primary* oder *secondary infringer* zu prüfen. Auch die Gesetzesbegründung legt diese Prüfungsreihenfolge nahe.[879] Da jedoch im Falle des Eingreifens einer der Safe-Harbor-Reglungen insbesondere jegliche Ansprüche des Rechtsinhabers auf Schadensersatz gegen den

873 H.R. Report No. 105-551 (I), S. 11 (1998).

874 S. Rep. 105-190, S. 19: *"Rather than embarking upon a wholesale clarification of these doctrines [of contributory and vicarious liability], the Committee decided to leave current law in its evolving state and, instead, to create a series of ‚safe harbors,' for certain common activities of service providers."*

875 Vgl. 8. Kapitel, Teil I. und II.

876 H.R. Rep. 105-551 (II), S. 50; Goldstein, § 6.3, 6:24 (2000); s.a. *Perfect 10 v. Cybernet Ventures*, 213 F. Supp. 2 d 1146, 1174 (C.D. Cal. 2002).

877 Vgl. beispielsweise *Ellison v. Robertson*, 357 F.3 d 1072, 1077 (9th Cir. 2004); *CoStar v. LoopNet*, 373 F.3 d 544, 553-555 (4th Circuit 2004).

878 S. Rep. 105-190, S. 19; *Perfect 10 v. CCBill*, 488 F.3 d 1102, 1109 (9th Cir. 2007); *Darrow/ Ferrera, 6 Nw. J. Tech. & Intell. Prop. 1,*, 6 Nw. J. Tech. & Intell. Prop. 1, 26 (2007). Zu den Rechtsfolgen, die das Eingreifen der Haftungsbeschränkung nach sich zieht, vgl. nachfolgendes Kapitel.

879 S. Rep. 105-190, S. 19: *"... Subsection 512 is not intended to imply that a service provider is or is not liable as an infringer either for conduct that qualifies for a limitation of liability or for conduct that fails to so qualify. Rather, the limitations of liability apply if the provider is found to be liable under existing principles of law."*

ISP vollumfänglich ausgeschlossen sind, d.h. es insoweit keine Rolle mehr spielt, ob eine Haftung des ISPs dem Grunde nach überhaupt gegeben ist, wird das Eingreifen der Haftungsbeschränkungen von vielen Gerichten an erster Stelle und damit noch vor der Haftung des ISPs dem Grunde nach geprüft.[880]

b. Ausschluss proaktiver Überwachungspflichten zu Lasten von ISPs

Wie dargelegt wurde, hielt man zum Zeitpunkt der Einführung der Haftungsbeschränkungen in § 512 eine uneingeschränkte Haftung von ISPs für Rechtsverletzungen der Nutzer ihrer Internetdienste aufgrund der technischen Gegebenheiten nicht für zumutbar.[881] Denn aufgrund des riesigen Datenaufkommens, das im Rahmen ihrer Internetdienste tagtäglich abgewickelt wurde, ging man davon aus, dass ISPs rein technisch nicht in der Lage waren, ihre Internetdienste effektiv zu überwachen und Rechtsverletzungen der Nutzer zu verhindern:

> „Billions of bits of data flow through the Internet and are necessarily stored on servers throughout the network and it is thus practically impossible to screen out infringing bits from noninfringing bits."[882]

Aus diesem Grund hielt es der Gesetzgeber für geboten, die Last des *copyright policing* in erster Linie den Rechtsinhabern aufzuerlegen und ISPs grundsätzlich von einer Verpflichtung, ihre Internetdienste auf Rechtsverletzungen zu überwachen, freizusprechen.[883] Dementsprechend wurde den Rechtsinhabern im Rahmen

880 Vgl. beispielsweise *IO Group, Inc. v. Veoh Networks, Inc.*, 2008 U.S. Dist. LEXIS 65915, *18; *Corbis Corp v. Amazon.com, Inc.,* 351 F. Supp.2 d 1090, 1098 (W.D. Wa. 2004); *CoStar Group, Inc. v. Loopnet, Inc.*, 164 F. Supp.2 d 688, 699 (D. Md. 2001): *„On summary judgement, it is often appropriate for a court to decide issues out of the traditional order because a dispute of facts is only material if it can affect the outcome of proceeding."*

881 S. Rep. 105-190, S. 8: *"...,without clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet. In the ordinary course of their operations service providers must engage in all kinds of acts that expose them to potential copyright infringement liability."*; vgl. 8. Kapitel, Teil B.III.2.b.

882 *Religious Technology Center v. Netcom On-Line Communication Services*, *Inc.*, 907 F. Supp. 1361, 1372-73 (N.D. Cal. 1995); *Bretan*, 18 Berkeley Tech L.J. 43, 44 (2003); *Zarins*, 92 Calif. L. Rev. 257, 274 (2004); die Ansicht der Unkontrollierbarkeit der Datenströme im Internet wurde im Gesetzgebungsverfahren zum DMCA verständlicherweise vor allem von den Vertretern der ISPs, wie z.B. AOL und Compuserve, vertreten, vgl. *Dimitrieva*, 16 Santa Clara Computer & High Tech. L.J. 233, 245 (2000).

883 *VerSteeg*, 9 N.C. J.L. & Tech. 43, 58: *"The drafter's goal was to make sure the ISPs would not be liable for copyright infringement under most circumstances, because there is no realistic way they can monitor everything that users post on the Internet. ... Under the DMCA, ISPS are not required to monitor their sites for copyright infringement, but, in the event that a copyright owner notifies an ISP of infringing activity, the ISP is required to remove that allegedly infringing content within a reasonable period of time."*; *Katyal*, 32 Colum. J.L. & Arts 401, 405 (2009).

des Notice&Takedown-Verfahrens gemäß § 512(c)(3) die Aufgabe auferlegt, die im Internet vorhandenen digitalen Inhalte nach Inhalten zu durchsuchen, die ihre Urheberrechte verletzen, und die ISPs hiervon in Kenntnis zu setzen. Erst aufgrund einer solchen Benachrichtigung sind die ISPs im Anschluss daran zur Beseitigung dieser Inhalte verpflichtet.[884]

Weiterhin wurde in § 512(m)(1) ausdrücklich klargestellt, dass ISPs grundsätzlich, d.h. außer im Zusammenhang mit einer „standard technical measure", die solche Kontrollmöglichkeiten eröffnet,[885] in keiner Weise dazu verpflichtet sind, zur Verhinderung von Urheberrechtsverletzungen ihre Internetdienste zu überwachen bzw. darin aktiv nach Umständen zu suchen, die das Vorliegen einer Urheberrechtsverletzung nahelegen.[886] Zwar dient diese Vorschrift ausweislich ihrer Überschrift („protection of privacy") in erster Linie dem Schutz der Privatsphäre. Sie soll somit vor allem sicherstellen, dass ISPs nicht um des Urheberschutzes willen investigative Maßnahmen ergreifen, die die berechtigten Erwartungen der Nutzer betreffend die Wahrung ihrer Privatsphäre beeinträchtigen.[887] Allerdings wird die Geltung des Ausschlusses proaktiver Überwachungspflichten auch außerhalb des Kontexts des Schutzes der Privatspähre der Nutzer in den Gesetzgebungsmaterialien wiederholt bekräftigt. So heißt es im Zusammenhang mit den Ausführungen zu den subjektiven Anforderungen, die ein ISP gemäß § 512(c)(1)(A) erfüllen muss, wenn er sich auf die Haftungsbeschränkung berufen will:[888]

> "As stated in new subsection (c)(l), a service provider need not monitor its service or affirmatively seek facts indicating infringing activity (except to the extent consistent with a standard technical measure complying with new subsection (h)), in order to claim this limitation on liability."[889]

Sowie weiterhin im Zusammenhang mit der generellen Anwendungsvoraussetzung der „repeat infringers policy":[890]

> "… the Committee does not intend this provision to undermine the principles of new subsection (l) or the knowledge standard of new subsection (c) by suggesting that a provider must investigate possible infringements, monitor its

884 Vgl. 8. Kapitel, Teil B.III.4.f.
885 Vgl. 8. Kapitel, Teil B.III.4.a.bb.
886 H.R. Rep. 105-551 (II), S. 64: *"... the applicability of new subsections (a) through (d) is in no way conditioned on a service provider: (1) monitoring its servcie or affirmatively seeking fracts indicating infringing activity except to the extent consistent with implementing a standard technical measure… ."*
887 *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.09[B], 12B-98.2 ff.
888 Vgl. 8. Kapitel, Teil III.4.d.
889 H.R. Rep. 105-551(II), S. 53.
890 Vgl. 8. Kapitel, Teil B.III.4.a.aa.

service, or make difficult judgments as to whether conduct is or is not infringing."[891]

Es ist daher davon auszugehen, dass im Rahmen von § 512 generell keine Verpflichtung von ISPs zu proaktiven Überwachungsmaßnahmen besteht.[892]

Dies bedeutet jedoch auch, dass Maßnahmen, die ein ISP zum Zwecke der Verbesserung der Kontrolle über die innerhalb seines Internetdienst stattfindenden Aktivitäten *freiwillig* ergreift, grundsätzlich nicht zu seinen Lasten gehen dürfen.[893] Denn ISPs sollten gerade dazu angespornt werden, technische Lösungen zum Schutz von Urheberrechten zu entwickeln und in ihren Internetdiensten einzusetzen. Dieses Ziel würde jedoch unterlaufen, wenn ISPs für ihre freiwilligen Bemühungen in dieser Hinsicht im Ergebnis dadurch bestraft werden würden, dass sie den Schutz der Safe-Harbor-Regelungen verlieren. Sowohl in der Ausgestaltung des Notice&Takedown-Verfahrens als auch in der Regelung betreffend Überwachungspflichten spiegelt sich somit die Bemühung des Gesetzgebers, die Möglichkeiten der Rechtsinhaber und der ISPs betreffend die Kontrolle von im Internet stattfindenden Urheberrechtsverletzungen unter Berücksichtigung der technischen Gegebenheiten in einen fairen, praktisch umsetzbaren und zukünftige Entwicklungen möglichst nicht beeinträchtigenden Ausgleich zu bringen.[894]

c. Rechtsfolgen der Anwendbarkeit der Safe-Harbor-Regelungen

Folge des Eingreifens der Haftungsbeschränkungen ist zunächst, dass finanzielle Entschädigungsansprüche („monetary damages") aller Art gegen den ISP grundsätzlich ausgeschlossen sind. Dabei erfassen *monetary damages* neben Schadensersatzansprüchen auch alle weiteren auf eine Geldleistung gerichteten Ansprüche, wie beispielsweise Ansprüche auf Erstattung von Kosten oder Anwaltsgebühren.[895]

Zudem ist die Gewährung von Abhilfe zugunsten der Rechtsinhaber in Form von „injunctions", d.h. in Form des Erlasses einer gerichtlichen Handlungs- oder

891 H.R. Rep. 105-551(II), S. 61.
892 *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.02[B][3], 12B-39; *Reese*, 34 Sw. U. L. Rev. 287, 294 (2004); *Manekshaw*, 10 Comp. L. Rev. & Tech. J. 101, 118-19 (2005); *Katyal*, 32 Colum. J.L. & Arts 401, 406 (2009).
893 H.R. Conf. Rep. 105-796, S. 73: *„This legislation is not intended to discourage the service provider from monitoring ist service for infringing material. Courts should not conclude that the service provider loses eligibility for limitations on liability under section 512 solely because it engaged in a monitoring program."*; *Bretan*, 18 Berkeley Tech L.J. 43, 44 (2003); *Reese*, 34 Sw. U. L. Rev. 287, 294 (2004).
894 *Goldstein*, Copyright, 2005, § 6.3.1, 6:26.
895 Vgl. 17 U.S.C. § 512(k)(2).

Unterlassungsverfügung, gemäß § 512(j)[896] nur unter bestimmten Voraussetzungen und in beschränktem Umfang zulässig.[897] Unabhängig davon, welche Fallgruppe der Safe-Harbor-Regelung im konkreten Fall eingreift, darf eine solche Verfügung grundsätzlich nur unter der Voraussetzung ergehen, dass der betroffene ISP zuvor von dem Begehren des Rechtsinhabers in Kenntnis gesetzt und ihm insoweit rechtliches Gehör gewährt wurde.[898] Auch muss das Gericht in jedem Fall die technischen und ökonomischen Belastungen der Betroffenen gegeneinander abwägen, die mit der Gewährung oder der Ablehnung einer *injunction* einhergehen.[899] Weiterhin muss das Gericht die Effektivität einer Maßnahme berücksichtigen. So fehlt beispielsweise dann die Rechtfertigung für den Erlass einer *injunction* unter dem Aspekt der Effektivität, wenn das betreffende rechtswidrige Material im Internet derart weitverbreitet ist, dass dessen Sperrung innerhalb des Internetdienstes des Antragsgegners der *injunction* auf die Rechtsverletzung praktisch keinen Einfluss hätte.[900]

In Bezug auf die Safe-Harbor-Regelung für Host-Provider gemäß § 512(c), die für Web 2.0-Dienste maßgeblich ist,[901] gibt das Gesetz drei Arten zulässiger gerichtlicher Verfügungen vor, die gegen den ISP erlassen werden können.[902] Zum einen kann der ISP zur Sperrung des Zugangs zu konkretem rechtsverletzendem Material oder zu einer bestimmten rechtswidrigen Aktivität innerhalb seines Systems verpflichtet werden. Zum anderen kann ihm auferlegt werden, das Nutzerkonto und damit die Zugangsberechtigung eines bestimmten, in der Anordnung bezeichneten Nutzers, der eine Rechtsverletzung begangen hat, zu seinem Internetdienst zu beendigen. Darüber hinaus erlaubt das Gesetz die Anordnung aller

896 Vgl. 17 U.S.C. § 512(j).

897 *Perfect 10 v. Amazon.com*, 487 F.3 d 701, 714 (9th Cir. 2007): *„A service provider that qualifies for such protection ... may be subject only to the narrow injunctive relief set forth in section 512(j).“*

898 17 U.S.C. § 512(j)(3); *Goldstein*, Copyright, 2005, § 6.3.1, 6:39.

899 17 U.S.C. § 512(j)(2); *Goldstein*, Copyright, 2005, § 6.3.1, 6:40; *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.11[B], 12B-133.

900 *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.11[A][2], 12B-134.

901 Vgl. 8. Kapitel, Teil B.III.4.

902 Vgl. 17 U.S.C. § 512(j)(1): *„Scope of relief. (A) With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a service provider only in one or more of the following forms:*
(i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network.
(ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.
(iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.“

weiterer Maßnahmen, die nach Ansicht des Gerichts notwendig sind, um die Verletzung eines urheberrechtlich geschützten Werks durch in der Anordnung genau bezeichnetes, im Internet befindliches Material effektiv zu unterbinden. Solche Maßnahmen müssen jedoch verhältnismäßig sein, d.h. sie müssen die jeweils mildeste Alternative unter den zur Verfügung stehenden Mitteln darstellen.[903] Folglich kann eine Maßnahme gegen einen ISP beispielsweise dann nicht ergehen, wenn es auch möglich wäre, die Urheberrechtsverletzung durch ein Vorgehen gegen den unmittelbaren Rechtsverletzer abzustellen.[904] Durch diese detaillierten gesetzlichen Vorgaben wird das Ermessen der Gerichte auf Rechtsfolgenseite weitgehend reduziert um sicherzustellen, dass die durch das Gericht erlassene *injunction* die technischen und wirtschaftlichen Gegebenheiten des Internets ausreichend berücksichtigt.[905]

4. Die Tatbestandsvoraussetzungen der Haftungsbeschränkung für Host-Provider gemäß 17 U.S.C. § 512(c)

> „New Section 512(c) limits the liability of qualifying service providers for claims of direct, vicarious and contributory infringement for storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider. ..".[906]

Die für Web 2.0-Dienste wie YouTube, Hulu oder MySpace einzig in Frage kommende Haftungsbeschränkung ist § 512(c), die Safe-Harbor-Regelung für sogenannte Host-Provider. Demnach wird die Haftung von ISPs beschränkt, deren internetbasierte Dienstleistung darin besteht, auf Anweisung der Nutzer Inhalte in einem von ihnen bereitgestellten System oder Netzwerk zu speichern.[907] Die Voraussetzungen dieser Haftungsbeschränkung werden nachfolgend dargestellt sowie die Auswirkungen von Content-Identification-Technologien auf deren Anwendbarkeit auf Web 2.0-Dienste geprüft.

903 *Goldstein*, Copyright, 2005, § 6.3.1, 6:41.
904 *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.11[A][2], 12B-132.
905 *Pankoke*, Von der Presse- zur Providerhaftung, 2000, S. 174.
906 H.R. Rep. 105-551 (II) S. 53.
907 *„...storage at the direction of a user of material that resides on a system or network controlled or operated by and for the service provider..."*.

a. Die „threshold conditions" gemäß 17 U.S.C. § 512(i)

Grundsätzliche Voraussetzung dafür, dass sich ein ISP auf die Safe-Harbor-Regelungen gemäß § 512 berufen kann, ist, dass er die in § 512(i)(1)[908] niedergelegten Bedingungen (sogenannte „treshold conditions")[909] erfüllt. Demnach müssen ISPs im Rahmen ihrer Internetdienste eine „repeat infringers policy" unterhalten und weiterhin „standard technical measures" innerhalb ihrer Internetdienste einsetzen. Diese beiden Bedingungen müssen unabhängig davon erfüllt sein, welche der vier Safe-Harbor-Regelungen auf einen konkreten Sachverhalt anwendbar ist. Da der Schutz der Safe-Harbor-Regelung von vornherein ausscheidet, wenn ein ISP die *threshold conditions* nicht erfüllt, wird ihr Vorliegen noch vor den Tatbestandsvoraussetzungen der potentiell einschlägigen Safe-Harbor-Regelung geprüft.[910]

aa. Repeat infringers policy

Zum einen muss der ISP gemäß § 512(i)(1)(A) für seinen Internetdienst Richtlinien aufgestellt haben, in denen der Umgang mit Nutzern, die seinen Internetdienst wiederholt zu rechtswidrigen Verhaltensweisen nutzen („repeat infringers"), geregelt ist. Gleichzeitig muss gewährleistet sein, dass diese Richtlinien in der Praxis auch in gehörigem Umfang umgesetzt werden. § 512(i)(1)(A) verfolgt mit solchen seitens der ISPs zu ergreifenden Maßnahmen das Ziel, auf Seiten der Nutzer ein Bewusstsein dafür zu schaffen, dass eine konkrete Gefahr besteht, den Zugang zu einem Internetdienst zu verlieren, wenn dieser wiederholt oder „in schamloser Weise" zur Verletzung von Urheberrechten missbraucht wird.[911] Allerdings sollen dadurch weder die subjektiven Anforderungen der Haftungsbeschränkung gemäß § 512(c)[912] modifiziert werden, noch indirekt eine proaktive Überwachungspflicht zu Lasten von ISPs geschaffen werden.[913]

908 *„Conditions for Eligibility. (1) Accommodation of technology. The limitations on liability established by this section shall apply to a service provider only if the service provider (A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and (B) accommodates and does not interfere with standard technical measures."*

909 Vgl. beispielsweise *Perfect 10 v. CCBill*, 488 F.3 d 1102, 1109 (9th Cir. 2007).

910 Vgl. beispielsweise *Ellison v. Robertson*, 189 F. Supp. 2 d 1051, 1064 (C.D. Cal. 2002), bestätigt durch den Ninth Circuit in 357 F.3 d 1072, 1080 (9th Circuit 2004).

911 H.R. Rep. 105-551 (II) S. 61.

912 Vgl. 8. Kapitel, Teil B.III.4.d.

913 H.R. Rep. 105-551, S. 61; *Reese*, 34 Sw. U. L. Rev. 287, 297 (2004); vgl. hierzu auch die Ausführungen des Gerichts in *Perfect 10 v. CCBill*, 488 F.3 d 1102, 1111: *„To identify and*

Die inhaltlichen Anforderungen an die *repeat infringers policy*, die das Auftreten zukünftiger, wiederholter Rechtsverletzungen verhindern helfen soll, wurden vom Gesetzgeber – vor allem im Vergleich zu den ausführlichen inhaltlichen Vorgaben des Notice&Takedown-Verfahrens[914] – nur rudimentär ausgestaltet.[915] Teilweise wird vermutet, dass dies damit zu erklären ist, dass die grundsätzliche Entscheidung des Gesetzgebers, ISP eine wirkungsvolle Beschränkung ihrer Haftung zu gewähren, nicht durch zu hohe Anforderungen an die Ausgestaltung und Durchsetzung der *repeat infringer policy* untergraben werden sollte.[916] Aus diesem Grund soll zur Erfüllung dieser Voraussetzung ausreichen, dass ein ISP bei der Aufstellung der Richtlinien nach bestem Wissen und Gewissen gehandelt hat und dabei die wenigen vom Gesetzgeber explizit vorgegebenen Kriterien erfüllt.[917] Da § 512(i)(1)(A) zudem eine Reihe unbestimmter Rechtsbegriffe enthält, zu deren Auslegung das Gesetz selbst keine und die Gesetzesbegründung nur wenig Auskunft geben, ist davon auszugehen, dass die Anwendung der Vorschrift auf konkrete Sachverhalte noch einige Fragen aufwerfen wird.[918]

bb. Standard Technical Measures

Zudem muss ein ISP gemäß § 512(i)(1)(B) in seinem Internetdienst Technologien implementieren, die von den Rechtsinhabern zum Schutz oder zur Identifizierung ihrer Werke eingesetzt werden, sofern diese als *standard technical measures*

terminate repeat infringers, a service provider need not affiermatively police its users for evidence of repeat infringement. Section 512(c) states that „[a] service provider shall not be liable for monetary relief" if it does not know of infringement. A service provider is also not liable under § 512 (c) if it acts „expeditiously to remove, or disable access to, the material" when it (1) has actual knowledge, (2) is aware of facts or circumstances from which infringing activity is apparent, or (3) has received notification of claimed infringement meeting the requirements of § 512(c)(3). Were we to require service providers to terminate users under circumstances other than those specified in § 512(c), § 512(c)'s grant of immunity would be meaningless."

914 Vgl. 8. Kapitel, Teil B.III.4.f.

915 *Nimmer* in: Nimmer on Copyright, 2009, § 12B.10[A][1], 12B - 100.

916 *Nimmer* in: Nimmer on Copyright, 2009, § 12B.10[A][1], 12B – 122-23.

917 *Nimmer* in: Nimmer on Copyright, 2009, § 12B.10[A][1], 12B – 123. Einige Gerichte haben sich bereits mit dem Erfordernis der *repeat infringers policy* befasst, vgl. beispielsweise *Ellison v. Robertson*, 357 F.3 d 1072, 1077-80 (9th Circ. 2004); *In re Aimster Copyright Litigation*, 334 F.3 d 643, 655 (7th Cir. 2003); *Perfect 10 v. CCBill*, 488 F.3 d 1102, 1111 (9th Cir. 2007).

918 *Nimmer* beschäftigt sich ausgiebig mit der Frage, welche Anforderungen an eine gesetzeskonforme *repeat infringers policy* zu stellen sind, vgl. *Nimmer* in: Nimmer on Copyright, 2009, § 12B.10[A][1], 12B – 123-24.

(„STMs“) zu qualifizieren sind. Was unter einer STM im Einzelnen zu verstehen ist, wird in § 512(i)(2)[919] definiert:

> „As used in this subsection, the term „standard technical measures“ means technical measures that are used by copyright owners to identify or protect copyrighted works and (A) are developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process; (B) are available to any person on reasonable and nondiscriminatory terms; and (C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.“

(1) Gesetzgeberische Intention hinter § 512(i)(1)(B)

Aus der Gesetzesbegründung geht hervor, dass der Gesetzgeber mit der Einführung des Begriffs der STMs beabsichtigte, eine branchenübergreifende Anstrengung zur Entwicklung geeigneter Technologien zum Schutz von Urheberrechten im Rahmen von Internetdiensten anzustoßen.[920] Denn zum Zeitpunkt der Schaffung der Haftungsbeschränkungen ging der Gesetzgeber davon aus, dass viele der Probleme, die sich aus der Digitalisierung in Bezug auf den urheberrechtlichen Schutz von Multimediawerken ergeben, in Zukunft auf technologischem Wege gelöst werden würden.[921] Um den Fortschritt in diesem Bereich anzuspornen, entschied sich der Gesetzgeber, solche zukünftigen technischen Entwicklungen in Form des Konstrukts der STMs ausdrücklich in den *Copyright Act* einzubeziehen. Da zum Zeitpunkt der Einführung dieser Regelung jedoch solche Technologien noch nicht existierten,[922] wurden die betroffenen Interessengruppen vom Gesetzgeber parallel dazu aufgerufen, möglichst zeitnah in einen industrieübergreifenden Diskurs mit dem Ziel einzutreten, sich auf den am besten geeigneten technischen Ansatz zur

919 *„As used in this subsection, the term „standard technical measures“ means technical measures that are used by copyright owners to identify or protect copyrighted works and (A) are developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process; (B) are available to any person on reasonable and nondiscriminatory terms; and (C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.“*

920 H.R. Rep. 105-551 (II), S. 61; *Reese*, 34 Sw. U. L. Rev. 287, 293-94 (2004).

921 *Dimitrieva*, 16 Santa Clara Computer & High Tech. L.J. 233, 240 (2000); *Goldstein*, Copyright, 2005, § 6.3.1, 6:29; *Nimmer*, 16 Berkeley Tech. L.J. 855, 864 (2001).

922 Da somit das Gesetz mit dem Begriff der STMs auf etwas Bezug nimmt, was zum Zeitpunkt des Gesetzeserlasses noch nicht existierte und zu diesem Zeitpunkt auch nicht absehbar war, dass solche Technologien jemals zur Entstehung gelangen würden, wurde dieses Element der Safe-Harbor-Regelung auch schon als die „kurioseste Eigentümlichkeit“ des Gesetzeswerks bezeichnet, vgl. *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.01[C][4], 12B – 28.

Lösung des Problems des Urheberschutzes im Internet zu einigen und in der Praxis umzusetzen.[923]

(2) Maßgeblichkeit des Verfahrens, in dem eine Technologie entwickelt wurde, für die Qualifizierung als STM

Maßgeblich für die Qualifizierung einer Technologie als STM ist, dass sie auf der Grundlage eines breiten Konsenses („broad consensus") zwischen Rechtsinhabern und ISPs in einem offenen, fairen, freiwilligen und industrieübergreifenden Verfahren (*„open, fair, voluntary, multi-industry standards process"*) entwickelt wurde.

Was genau unter der Vielzahl unbestimmter Rechtsbegriffe zu verstehen ist, die das Verfahren beschreiben, in dessen Rahmen STMs entwickelt werden müssen, wird im Gesetz nicht näher erläutert. Bisher existiert auch kein *case law*, das sich mit den Voraussetzungen, die zur Entstehung einer STM führen, im Einzelnen auseinandersetzt. Daher besteht erhebliche Unsicherheit darüber, wann eine neue Technologie als STM zu qualifizieren ist und – aufgrund der Eigenschaft von § 512(i)(1)(B) als *threshold requirement* für die Anwendbarkeit der Haftungsbeschränkungen auf einen ISP – damit gleichzeitig, wann die Anwendbarkeit der Safe-Harbor-Regelung auf einen ISP vom Einsatz einer solchen Technologie im Rahmen seines Internetdienstes abhängig ist.[924]

Auch ist unklar, was mit dem *broad consensus* der Betroffenen gemeint ist, auf dessen Grundlage STMs geschaffen sein müssen. Da dieser Begriff auch nicht an anderer Stelle im US-amerikanischen Urheberrecht verwendet wird, existieren insoweit keinerlei Anhaltspunkte dafür, wie diese Voraussetzung inhaltlich auszulegen ist. Grundsätzlich versteht man unter dem Konsensprinzip, dass für die Zustimmung zu einer Entscheidungsalternative nicht eine ausdrücklich erklärte Einstimmigkeit der Abstimmenden erforderlich ist, sondern nur, dass keiner der Abstimmenden der Entscheidung ausdrücklich widerspricht.[925] Übertragen auf die Auslegung von § 512(i)(2) bedeutet dies, dass für das Vorliegen von STMs erfor-

923 H.R. Rep. 105-551 (II), S. 61.

924 *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.01[C][4], 12B – 28-29.

925 Black's Law Dictionary, 2009: *„Consensus: A general agreement; collective opinion. … 'The regular method for the chair to use is to aks the members 'Is it the consensus of this meeting that … is agreed to?' or, 'is it the will of the assembly that … is agreed to?' or, 'Is there an objection?' Consensus has been used successfully throughtout the years by Quakers, Indians, New England town meetings, and others as a decision-making procedure. It permits compromise. In small groups where less formality is required, it is a simple method for making decisions – "General consent is an equivalent to consensus, when done without objection. Otherwise, a formal vote must be taken." Floyd M. Riddick & Miriam H. Butcher,*

derlich ist, dass kein Rechtsinhaber oder ISP der Entwicklung der als STM zu qualifizierenden Technologie ausdrücklich widersprochen hat. Durch Hinzufügung des Attributs „broad" wird weiterhin klargestellt, dass eine Technologie sich auch trotz des Widerspruchs einzelner als STM qualifizieren kann, solange der Konsens trotz dieses Widerspruchs einiger weniger weiterhin als eine Übereinstimmung der weit überwiegenden Mehrheit anzusehen ist.

(3) Weitere Kriterien

Die als STM zu qualifizierende Technologie muss von den Rechtsinhabern zu dem Zweck eingesetzt werden, dessen urheberrechtlich geschützte Werke zu identifizieren oder zu schützen. Darüber hinaus ist erforderlich, dass ihre Nutzung jedem ISP zu angemessenen und fairen Bedingungen offensteht. Dies bedeutet, dass die Verpflichtung zum Einsatz der Technologie nicht dazu führen darf, dass einzelne ISPs im Wettbewerb mit anderen dadurch diskriminiert werden, dass sie an die Technologie nur unter einem erhöhten Kostenaufwand oder zu nachteiligen Bedingungen „herankommen". Auch dürfen durch die Technologie dem ISP keine unzumutbaren Kosten bzw. dessen technischen Systemen keine unzumutbaren Belastungen aufgebürdet werden.

(4) STMs als Ausnahme vom Ausschluss allgemeiner Überwachungspflichten zu Lasten von ISPs

Technologien, die sich entsprechend den vorgenannten Kriterien als STMs qualifizieren, können auch dazu führen, dass ISPs mit ihrer Hilfe ihre Internetdienste auf Urheberrechtsverletzungen überwachen müssen. Dies ergibt sich aus § 512(m), wonach der Grundsatz, dass ISPs nicht zur proaktiven Überwachung ihrer Internetdienste verpflichtet sind[926] mit der Maßgabe gilt, dass eine solche Überwachung im Zusammenhang mit dem Einsatz von STMs möglich wird.[927] Eine Verpflichtung für ISPs zur proaktiven Überwachung ihrer Internetdienste kann somit aus-

Riddick's Rules of Procedure 56 (1985)."; "General consent: 1. Adoption without objection, regardless of whether every voter affirmatively approves. 2. See unanimous consent (1):." "Unanimous consent: 1. Adoption with every voter's approval. 2. see general consent (1)".

926 Vgl. 8. Kapitel, Teil B.III.3.b.

927 H.R. Rep. 105-551 (II), S. 53: *„As stated in new subsection (c)(l)* [Anmerkung der Verfasserin: entspricht § 512(m)(1) in der endgültigen Fassung des DMCA] *a service provider need not monitor its service or affirmatively seek facts indicating infringing activity (except to the extent consistent with a standard technical measure complying with new subsection (h)), in order to claim this limitation on liability...".*

nahmsweise dadurch entstehen, dass Technologien, die die Voraussetzungen einer STM gemäß § 512(i)(2) erfüllen, eine solche Überwachung ermöglichen.[928]

cc. Bewertung: Auswirkungen von Content-Identification-Technologien auf das Vorliegen der threshold requirements gemäß § 512(i)(1) in Bezug auf Web 2.0-Dienste

Für die Zwecke dieser Arbeit wird vorausgesetzt, dass der jeweilige Web 2.0-Dienst eine die gesetzlichen Anforderungen erfüllende *repeat infringers policy* entwickelt hat und diese im Rahmen seines Internetdienstes auch entsprechend durchsetzt. Zu prüfen bleibt somit, ob Content-Identification-Technologien sich möglicherweise als STMs im Sinne von § 512(i)(1)(B) qualifizieren lassen. Wäre dies zu bejahen, wäre der Einsatz einer solchen Technologie durch den Betreiber eines Web 2.0-Dienst zwingende Voraussetzung für die Anwendbarkeit der Safe-Harbor-Regelung gemäß § 512(c).

(1) Prüfung einer möglichen Qualifizierung von Content-Identification-Technologien als STMs

(i) Allgemeine Anforderungen

Wie gezeigt wurde, ist nach der Legaldefinition gemäß § 512(i)(2) zur Qualifizierung einer Technologie als STM zunächst erforderlich, dass diese von den Rechtsinhabern zur Identifikation oder zum Schutz ihrer urheberrechtlich geschützten Werke eingesetzt wird. Diese Anforderung ist in Bezug auf Content-Identification-Technologien ohne weiteres zu bejahen. Denn mit Hilfe dieser Technologien können die Rechtsinhaber digitale Kopien ihrer urheberrechtlich geschützten Werke in Internetdiensten identifizieren. Darüber hinaus wird den Rechtsinhabern ermöglicht, ihre Urheberrechte durchzusetzen, entweder indem sie die unautorisierte Nutzung ihrer Werke durch Entfernung der Kopien aus den jeweiligen Internetdiensten gänzlich unterbinden oder indem sie die Nutzung ihrer Werke – beispielsweise durch die Hinzuschaltung von Werbung – kommerzialisieren.[929]

Weiterhin müssten Digital-Fingerpinting-Technologien in einem offenen, fairen, freiwilligen und industrieübergreifenden Verfahren entwickelt worden sein. Insoweit ist bereits problematisch, dass es derzeit nicht „die eine" Content-Identification-Technologie gibt, sondern eine Vielzahl unterschiedlicher, von verschie-

928 *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.02[B][3], 12B-39.
929 Vgl. 7. Kapitel, Teil C.

denen Anbietern entwickelten Technologien.[930] Diese unterschiedlichen Technologien eint zwar, dass sie auf dem Prinzip der Identifikation von urheberrechtlich geschützten Werken auf Grundlage eines digitalen Fingerabdrucks des jeweiligen Multimediawerks und damit auf einer *perceptual hash function*[931] basieren. Jedoch sind die insoweit verwendeten Algorithmen und Ansätze je nach Anbieter und in Abhängigkeit von dem speziellen Einsatzgebiet, auf das die jeweilige Technologie zugeschnitten ist, sehr verschieden. Auch handelt es sich bei den Anbietern allesamt um private Technologieunternehmen, die mit der Entwicklung und dem Vertrieb dieser Technologien ihre individuellen wirtschaftlichen Zwecke verfolgen. Es gibt daher bisher keine Content-Identification-Technologie, die in einem den gesetzlichen Anforderungen entsprechenden Verfahren entwickelt worden wäre.

(ii) Mögliche Auswirkungen der UGCP-Initiative auf die Qualifizierung von Content-Identification-Technologien als STMs

Vor dem Hintergrund des *threshold requirement* gemäß § 512(i)(1)(B) erscheint jedoch die UGCP-Initiative[932] ein einem neuen Licht. Es ist zu vermuten, dass der eigentliche Beweggrund der Rechtsinhaber hinter dieser Initiative darin liegt, hierdurch die gesetzlichen Voraussetzungen zur Qualifizierung von Content-Identification-Technologien als STMs herbeizuführen. Denn würde dieses Ziel erreicht, wären ab sofort alle Web 2.0-Dienste unabhängig von ihrer Teilnahme an der UGCP-Initiative gemäß § 512(i)(1)(B) zum Einsatz von Content-Identification-Technologien gezwungen, sofern sie die Haftungsbeschränkung gemäß § 512(c) weiterhin beanspruchen wollen. Damit wären die Web 2.0-Dienste jedoch gleichzeitig verpflichtet, ihre Internetdienste in Bezug auf Urheberrechtsverletzungen zu überwachen und zu durchsuchen, soweit dies durch die jeweilige Content-Identification-Technologie möglich wird. Damit hätten die Rechtsinhaber ihr Hauptziel erreicht, nämlich die Last des *copyright policing* auf die ISPs überzuwälzen.

Voraussetzung hierfür wäre jedoch, dass sich ein weit überwiegender Teil der ISPs der UGCP-Initiative anschließen und sich gemeinsam mit den Rechtsinhabern auf eine bestimmte Content-Identification-Technologie einigen würde, die innerhalb von Web 2.0-Diensten eingesetzt werden sollen, und diese Technologie anschließend in einem offenen, fairen, freiwilligen und interdisziplinären Standardisierungsverfahren entwickelt werden würde. Erst dann wären die Anforderungen, die § 512(i)(2) an die Entwicklung von STMs stellt, erfüllt. Allerdings ist aufgrund der Folgen, die im Falle einer Qualifizierung von Content-Identification-Techno-

930 Vgl. 7. Kapitel, Teil B.
931 Vgl. 7. Kapitel, Teil B.I.
932 Vgl. 8. Kapitel, Teil A.I.

logien als STMs die ISPs treffen würden, unwahrscheinlich, dass sich die weit überwiegende Mehrheit der ISPs den UGCP anschließen wird. Denn nach der derzeitigen Rechtslage befinden sich ISPs aufgrund der grundsätzlichen Entscheidung des Gesetzgebers, ihnen keine Überwachungspflichten aufzubürden, in einer sehr komfortablen Situation, indem es die Rechtsinhaber sind, die den zeitlichen und finanziellen Aufwand des *copyright policing* hauptsächlich zu tragen haben. Daher empfinden ISPs wie Google und Yahoo im Gegensatz zu den Rechtsinhabern die gegenwärtige Rechtslage als „perfekt", [933] weswegen sie keinen Anreiz dafür sehen dürften, hieran etwas zu ändern. Insbesondere dürften diese ISPs offensichtlich kein Interesse daran haben, aufgrund ihrer Mitwirkung an der UGCP-Initiative die Voraussetzungen dafür zu schaffen, dass sie sich künftig nur unter der Bedingung des Einsatzes einer bestimmten Content-Identification-Technologie innerhalb ihrer Internetdienste auf die Safe-Harbor-Regelungen berufen können. Auch verstärkt die derzeitige Rechtslage die Verhandlungsposition der ISPs gegenüber den Rechtsinhabern. Denn da ihrerseits jegliche Maßnahmen zur Überwachung und Eindämmung von Rechtsverletzungen auf ihren Internetdiensten nach der geltenden Rechtslage auf freiwilliger Basis erfolgen, können die Rechtsinhaber als Gegenleistung für diese gesetzlich nicht geschuldeten und damit überobligatorischen Überwachungsmaßnahmen der ISPs faktisch zu entsprechenden Zugeständnissen bei der Einräumung von Rechten und der Frage der Höhe etwaiger Lizenzzahlungen gezwungen werden.[934] So erklärt sich auch das letztendliche Fernbleiben von Unternehmen wie Google und Yahoo von der UGCP-Initiative, obwohl beide Unternehmen an den Verhandlungen zur Ausarbeitung der UGCP beteiligt waren.[935]

Es ist daher zu erwarten, dass die ISPs ihrerseits alles dafür tun werden, um den Eintritt der Voraussetzungen für die Entstehung von STMs gemäß § 512(i)(2) zu verhindern.[936] Hieran zeigt sich deutlich der Schwachpunkt des Konstrukts der STMs. Denn nach der gesetzlichen Definition wird die Entstehung dieser *threshold condition* für die Anwendbarkeit der Safe-Harbor-Regelung vom Willen derjenigen abhängig gemacht, die hiervon negativ betroffenen würden. Damit werden die Betroffenen jedoch in die Lage versetzt, das Entstehen von STMs aus eigennützigen Motiven einseitig zu verhindern.[937] Somit können ISPs die an und für sich begrüßenswerte Absicht des US-amerikanischen Gesetzgebers, einen für die Zwecke des Urheberrechts wünschenswerten zukünftigen technischen Fortschritt au-

933 So *Daphne Keller*, derzeit Senior Products Counsel von Google Inc., sowie *Denelle Dixon-Thayer*, seinerzeit Senior Legal Director von Yahoo! Corp., auf einer Präsentation der Annual Conference 2009 der Deutsch-Amerikanischen Juristenvereinigung (DAJV) am 13.8.2009 in Berkeley.

934 *Meisel*, Journal of Internet Law 12/8 1, 10 (2009).

935 S.o.

936 *Cloak*, 60 Vand. L. Rev. 1559, 1583-84 (2007).

937 *Nimmer* in: Nimmer on Copyright, 2009, § 12B.02[B][3], 12B – 38.

tomatisch zu einer Veränderung des Umfangs der Überwachungspflichten von ISPs führen zu lassen, aus eigennützigen Motiven torpedieren. Aufgrund des Versäumnisses des Gesetzgebers, sicherzustellen, dass sich STMs auch unabhängig von gegenläufigen Einzelinteressen etablieren können,[938] wird damit im Ergebnis der hinter dem Konstrukt der STMs stehende Zweck verfehlt, die den ISPs gewährte weitgehende Haftungsbeschränkung im Falle der Entwicklung geeigneter Technologien zur besseren Kontrolle von Urheberrechtsverletzungen zu relativieren.

(2) Ergebnis

Aus den dargestellten Gründen scheidet eine Qualifizierung von Content-Identification-Technologien als STMs derzeit (noch) aus.[939] ISPs müssen daher keine Content-Identification-Technologien einsetzen, um die Anwendbarkeit des Safe-Harbor-Regelung gemäß dem *threshold requirement* in § 512(i)(1)(B) sicherzustellen.

b. Persönlicher Anwendungsbereich: „service provider"

Voraussetzung für die Eröffnung des persönlichen Anwendungsbereichs von § 512(c) ist, dass der jeweilige ISP die Merkmale eines „service provider" gemäß § 512(k)(1)(B) erfüllt.[940]

aa. Allgemeine Anforderungen

Im Zusammenhang mit § 512(b)-(d) gelten als *service provider* sämtliche Anbieter von Internetdiensten („online services") oder Netzwerkzugängen sowie Unternehmen, die die für solche Dienstleistungen erforderliche Infrastruktur bereitstellen.[941] Die Legaldefinition ist sehr weit gefasst und lässt erheblichen Auslegungs-

938 *Nimmer*, 16 Berkeley Tech. L.J. 855, 865 (2001): *„ ... Congress had legislated no teeth to see its precatory language thorugh to completion."*

939 *Darrow/Ferrera*, 6 Nw. J. Tech. & Intell. Prop. 1, 17 (2007).

940 *„Service Provider. (A) As used in subsection (a), the term 'service provider' means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."*
(B) As used in this section, other than subsection (a), the term 'service provider' means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).".

941 H.R. Rep. 105-551 (II), S. 64.

spielraum zu, beispielsweise in Bezug auf den Begriff der *online services*, der vom Gesetz nicht weiter eingegrenzt wird.[942] Aus der Gesetzesbegründung geht hervor, dass insbesondere die Anbieter von Emaildiensten, Chatrooms, Webseiten und anderen internetbasierten Dienstleistungen von der Definition erfasst werden; darüber hinaus beispielsweise aber auch private Unternehmen, die ein Intranet unterhalten.[943]

Weiterhin werden auch sämtliche Internetdienste, die als *service provider* im Sinne der eigens auf die Safe-Harbor-Regelung gemäß § 512(a) zugeschnittenen Definition gemäß § 512(k)(1)(A) gelten, von der Definition gemäß § 512(k)(1)(B) erfasst.[944] Demnach gilt als service provider, wer die Übermittlung von digitalen, über das Internet stattfindenden Kommunikationen in Bezug auf vom Nutzer ausgesuchtes Material anbietet oder die dafür notwendigen Verbindungen zur Verfügung stellt, wobei der Inhalt des im Rahmen des Kommunikationsvorgangs übermittelten Materials nicht verändert werden darf. Diese Definition wurde in Anlehnung an den im Communications Act verwendeten Begriff der „telecommunications" entwickelt und erfasst die klassischen Access-Provider.

bb. Auslegung durch die Gerichte

Entsprechend der gesetzlichen Vorgaben wurde der Begriff des *service provider* von den bisher damit befassten Gerichten weit ausgelegt.[945] So wurden bereits das Internetauktionshaus eBay sowie ein Unternehmen, das über das Internet Immobilienangebote veröffentlichte, als *service provider* im Sinne dieser Definition eingeordnet.[946] In *Perfect 10 v. Cybernet Ventures* vertrat das Gericht die Auffassung, dass aufgrund der Weite der Legaldefinition davon auszugehen sei, dass nahezu alle Betreiber von Webseiten im Internet unter die Definition subsumiert werden könnten.[947] In den beiden *Veoh*-Entscheidungen wurde die Eigenschaft des Betreibers einer Videoplattform als *service provider* im Rahmen der Prüfung der Anwendbarkeit der Safe-Harbor-Regelung vom Gericht nicht einmal mehr angesprochen, d.h. als offensichtlich gegeben vorausgesetzt.[948]

942 *Ginsburg*, 50 Ariz. L. Rev. 577, 593 (2008).
943 H.R. Rep. 105-551 (II), S. 64; *Nimmer* in: Nimmer on Copyright, 2009, § 12B.03[B][1], 12B-48, 12B-48.1; *Goldstein*, Copyright, 2005, § 6.3.1, 6:27 (2005).
944 Vgl. H.R. Rep. 105-551 (II), S. 63.
945 *Darrow/Ferrera*, 6 Nw. J. Tech. & Intell. Prop. 1, 13 (2007); *Reese*, 34 Sw. U. L. Rev. 287, 294 (2004).
946 *Hendrickson v. eBay*, Inc., 165 F. Supp. 2 d 1082, 1088 (C.D. Cal. 2001); *Costar Group Inc. v. Loopnet*, Inc., 164 F. Supp. 2 d 688, 701 (D. Md. 2001).
947 *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, F.Supp. 2 d 1044, 1175 (C.D.Cal. 2002).
948 *IO Group, Inc. v. Veoh Networks, Inc.*, 2008 U.S. LEXIS 65915 (N.D. Cal. 2008); *Universal Recordings, Inc. v. Veoh Networks Inc.,* 2009 U.S. Dist. LEXIS 86932 (C.D. Cal. 2009).

cc. Bewertung: Eröffnung des persönlichen Anwendungsbereichs in Bezug auf Web 2.0-Dienste

Aufgrund der weit gefassten gesetzlichen Definition und der entsprechend weiten Auslegung des Begriffs *service provider* durch die Gerichte ist davon auszugehen, dass Web 2.0-Dienste wie Videoplattformen oder soziale Netzwerke von einem Gericht in der Regel ohne weiteres als *service provider* im Sinne von § 512(k)(1)(A) eingeordnet werden würden.

c. Sachlicher Anwendungsbereich: „storage at the direction of a user"

§ 512(c) beschränkt die Haftung eines ISPs im Zusammenhang mit Urheberrechtsverletzungen, die im Zusammenhang mit der Speicherung von Material im System oder Netzwerk des ISPs auf Anweisung des Nutzers eintreten: *„...for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider. "*

aa. Allgemeine Anforderungen

Wie bereits dargelegt wurde, befreit die Safe-Harbor-Regelung gemäß § 512(c) ISPs nicht generell von der Haftung für Urheberrechtsverletzungen, sondern beschränkt lediglich die Folgen einer solchen Haftung im Zusammenhang mit *bestimmten Tätigkeiten*, die von ISPs typischerweise im Rahmen ihrer Internetdienste ausgeführt werden. Dementsprechend beschränkt § 512(c) die Folgen der Haftung eines ISPs für Urheberrechtsverletzungen, die im Zusammenhang mit der Speicherung von Material auf Anweisung eines Nutzers in einem vom *service provider* kontrollierten System oder Netzwerk begangen werden.[949] Maßgeblich für die Anwendbarkeit von § 512(c) ist, dass die Speicherung des rechtswidrigen Materials im System oder Netzwerk des *service providers* auf eine Anweisung des Nutzers und nicht auf eine eigene Entscheidung des *service providers* zurückgeht.[950] Der klassische Anwendungsfall der Haftungsbeschränkung ist die Zurver-

949 Vgl. 17 U.S.C. § 512(c): *„Information Residing on Systems or Networks at Direction of Users.*
(1) In general. A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider."

950 H.R. Rep. 105-551 (II) S. 53.

fügungstellung von Speicherplatz auf dem Server des *service providers* zum Zwecke der Einrichtung einer Webseite, eines Chatrooms oder eines anderen Forums, wobei der Nutzer in diesem Zusammenhang die Speicherung von Informationen und Inhalten auf dem Server anweisen kann.[951]

Die Anwendbarkeit von § 512(c) auf Web 2.0-Dienste wird von Rechtsinhabern regelmäßig aufgrund der Tatsache angegriffen, dass die Inhalte, die ein Nutzer auf den Server des *service providers* hochlädt, zunächst durch eine Software des *service providers* automatisiert in ein anderes Dateiformat umgewandelt werden, bevor sie gespeichert und auf dem Internetdienst zugänglich gemacht werden.[952] Aufgrund dieses Vorgangs erfolge die Speicherung der Inhalte jedoch nicht mehr ausschließlich auf Anweisung des Nutzers, sondern aufgrund einer davon unabhängigen Entscheidung des ISPs. Dem wird von Seiten der ISPs entgegengehalten, dass es sich bei der Umformatierung lediglich um einen automatisierten Prozess handele, den der Nutzer gleichzeitig mit dem Prozess des Hochladens in Gang setze. Weiterhin sei dieser Prozess eine technische Notwendigkeit für eine möglichst nutzerfreundliche Konsumierbarkeit der hochgeladenen Inhalte.

Insoweit vertrat das Gericht in *CoStar Group, Inc. v. Loopnet, Inc.* („CoStar v. Loopnet") – der Argumentation des ISPs folgend – die Auffassung, dass trotz eines solchen Zwischenschritts die Speicherung von Inhalten auf einem Internetdienst in erster Linie auf die Willensentscheidung der Nutzer zurückgehe.[953] Zu diesem Ergebnis kam das Gericht, obwohl im Rahmen dieses Internetdienstes die Inhalte der Nutzer sogar erst nach einer flüchtigen menschlichen Überprüfung durch die Mitarbeiter des *service providers* auf dem Internetdienst eingestellt wurden. Das Gericht befand jedoch, dass die Tätigkeit der Mitarbeiter insoweit lediglich eine für die Frage der Anwendbarkeit der Haftungsbeschränkung unbeachtliche bloße „Brückenfunktion" darstellen würde. Zu einem ähnlichen Ergebnis kam auch das Gericht in *IO Group v. Veoh Networks* („IO v. Veoh").[954]

bb. Bewertung: Eröffnung des sachlichen Anwendungsbereichs in Bezug auf Web 2.0-Dienste

Das besondere Merkmal von Web 2.0-Diensten liegt darin, dass die Nutzer innerhalb solcher Internetdienste Inhalte ihrer Wahl, d.h. insbesondere auch digitale Multimediawerke, speichern und der Öffentlichkeit zugänglich machen können.[955] Web 2.0-Dienste fungieren als Plattformen oder Foren, die von den Nutzern

951 H.R. Rep. s.o.; S. Rep. 105-190, S. 43.
952 Vgl. beispielsweise *IO Group v. Veoh Networks*, 2008 U.S. Dist. LEXIS 65915, *34.
953 *CoStar Group, Inc. V. LoopNet, Inc.*, 164 F.Supp.2 d 688, 702 (D. Md. 2001).
954 *IO Group, Inc. v. Veoh Networks, Inc.*, 2008 U.S. Dist. LEXIS 65915, *37-38.
955 Vgl. 7. Kapitel, Teil A.I.

entsprechend ihrer Interessen und der im Rahmen der vom ISP zur Verfügung gestellten technischen Funktionen gestaltet werden können, ohne dass der ISP in diesen Prozess inhaltlich steuernd eingreift. Der Prozess des Hochladens bzw. Speicherns eines Inhalts auf einem Web 2.0-Dienst wird einseitig vom Nutzer ausgelöst und vom ISP nicht – außer gegebenenfalls einer Umwandlung der hochgeladenen Dateien in das von dessen Internetdienst verwendeten Dateiformat – beeinflusst. Aus alldem geht hervor, dass die Tätigkeit von ISPs im Zusammenhang mit Web 2.0-Diensten in den sachlichen Anwendungsbereich von § 512(c) fällt. Neben dem persönlichen ist somit auch der sachliche Schutzbereich von § 512(c) in Bezug auf Web 2.0-Dienste eröffnet.

d. Subjektive Voraussetzungen gemäß § 512(c)(1)(A)

Gemäß § 512(c)(1)(A)[956] kann sich ein ISP nur auf den Schutz der Safe-Harbor-Regelung berufen, wenn er keine positive Kenntnis von der Rechtsverletzung hat und ihm auch keine Umstände bekannt sind, aufgrund derer das Vorliegen einer solchen Verletzung offensichtlich ist. Darüber hinaus bleibt der Schutz der Haftungsbeschränkung auch dann bestehen, wenn der ISP nach der Erlangung solcher Kenntnis das rechtswidrige Material unverzüglich aus seinem Internetdienst entfernt oder den Zugang hierzu sperrt.

aa. Die Anforderungen an die Kenntnis des ISPs im Einzelnen

(1) Positive Kenntnis

Aus der Formulierung von § 512(c)(1)(A)(i) geht eindeutig hervor, dass sich die positive Kenntnis nicht nur auf das Material oder die Handlung an sich, sondern auch auf dessen bzw. deren Rechtswidrigkeit beziehen muss.[957] Da jedoch der Nachweis von positiver Kenntnis gerade auch der Rechtswidrigkeit einer Handlung oder eines Inhalts in der Regel schwer zu führen ist, stellt der Gesetzgeber damit

956 *„A service provider shall not be liable... if the service provider- (A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material... .“*

957 Vgl. den Wortlaut der Vorschrift: *„...does not have actual knowledge that the material or an activity ... is infringing“*; *Reese*, 32 Colum. J.L. & Arts 427, 433 (2009); damit sind die Anforderungen an die Kenntnis des ISP im Rahmen von § 512(c) höher als im Rahmen der Haftung für *contributory infringement*, da hier die Kenntnis der Handlung an sich ausreicht, vgl. *Goldstein*, Copyright, 2005 § 6.1, 6:6, Fn. 1.

sehr hohe Anforderungen an den Verlust des Anspruchs auf die Haftungsbeschränkung.[958] Um den Rechtsinhabern den schwer zu führenden Nachweis der positiven Kenntnis etwas zu erleichtern, wurde das Notice&Takedown-Verfahren gemäß § 512(c)(3) eingeführt, anhand dessen die Rechtsinhaber einen ISP über das Vorliegen einer Urheberrechtsverletzung innerhalb seines Internetdienstes benachrichtigen können.[959] Wird ein ISP in dieser Weise formfehlerfrei über eine Urheberrechtsverletzung informiert, gilt die positive Kenntnis des ISPs von der Rechtsverletzung als erwiesen.[960]

(2) Umstandskenntnis

Gemäß § 512(c)(1)(A)(ii) verliert ein Internetdienstleister den Schutz der Safe-Harbor-Regelung auch dann, wenn ihm Tatsachen oder Umstände bewusst sind, aufgrund derer das Vorliegen einer Rechtsverletzung offensichtlich ist („Umstandskenntnis"). Diese Voraussetzung wird in der Gesetzesbegründung auch als „red flag"-Test bezeichnet.[961]

Hinter dieser Vorschrift steht die grundsätzliche Überlegung, dass ein ISP, auch wenn er grundsätzlich nicht dazu verpflichtet ist, seinen Internetdienst aktiv zu überwachen oder nach Umständen, die eine Urheberrechtsverletzung indizieren, zu durchsuchen,[962] angesichts offensichtlicher Rechtsverstöße dennoch tätig werden muss, um weiterhin den Schutz der Haftungsbeschränkung beanspruchen zu können.[963] Allerdings ist ebenso wie bei dem Erfordernis der positiven Kenntnis erforderlich, dass nicht nur die rechtswidrige Aktivität oder das rechtswidrige Material an sich, sondern gerade auch deren bzw. dessen Rechtswidrigkeit offensichtlich ist.[964]

Für den Verlust der Haftungsbeschränkung ist weiter erforderlich, dass der ISP trotz der Kenntnis von eklatanten Tatsachen, die auf rechtswidriges Verhalten hinweisen, nicht reagiert und den Betrieb seines Dienstes willentlich unverändert fortsetzt.[965] Der ISP haftet somit, wenn er die Augen vor offensichtlichen Rechtsverletzungen willentlich verschließt.[966] Im Rahmen der Beurteilung, ob seitens des

958 Vgl. *Breen, YouTube or YouLose?, 2007*, YouTube or YouLose?, 2007, S. 16.
959 Vgl. 8. Kapitel, Teil B.III.4.f.
960 *Corbis Corporation v. Amazon.Com, Inc.*, Case No. CV03-1415L (W.D.Wash. 2004), S. 25.
961 H.R. Rep. 105-551 (II), S. 54.
962 Vgl. § 512(m); 8. Kapitel. Teil B.III.2.c.
963 H.R. Rep. 105-551 (II), S. 53.
964 *Reese*, 32 Colum. J.L. & Arts 427, 434 (2009).
965 *Nimmer* in: Nimmer on Copyright, 2009, § 12B.04[A][1], 12B-53.
966 H.R. Rep. 105-551 (II), S. 53: *„Under this standard, a service provider would have no obligation to seek out copyright infringement, but it would not qualify for the safe harbor if it had turned a blind eye to ‚red flags' of obvious infringement."*

ISPs Umstandskenntnis gegeben ist, kommen sowohl objektive als auch subjektive Kriterien zum Tragen. So ist bei der Prüfung der Frage, ob dem ISP im relevanten Zeitpunkt konkrete, auf Urheberrechtsverletzungen hindeutende Tatsachen bewusst waren, auf die subjektive Wahrnehmung des ISPs abzustellen. Hingegen ist bei der Beurteilung, ob diese Tatsachen als *red flags* zu qualifizieren sind, d.h. als Umstände, aufgrund derer die Rechtswidrigkeit des Materials oder des Verhaltens des Nutzers für eine vernünftige, unter gleichen Umständen agierende Person offensichtlich gewesen wäre, ein objektiver Maßstab anzulegen.[967]

Entsprechend dieser Vorgaben sind unter *red flags* im Sinne von § 512(c)(1)(A)(ii) Internetangebote zu verstehen, deren Rechtswidrigkeit durch die Verwendung eindeutiger Bezeichnungen wie beispielsweise „pirate", „bootleg" oder ähnliches offensichtlich und daher auch bei nur flüchtiger Betrachtung ohne weiteres erkennbar ist.[968] Dieses Verständnis von *red flags* trägt dem Umstand Rechnung, dass es gerade im Internetkontext mitunter erhebliche Schwierigkeiten bereiten kann, die Rechtswidrigkeit der konkreten Nutzung eines urheberrechtlich geschützten Multimediawerks mit Sicherheit festzustellen.[969] Ziel des Gesetzgebers war es insoweit, ISPs davor zu bewahren, schwierige rechtliche Einschätzungen bezüglich der Rechtswidrigkeit einzelner Internetangebote treffen zu müssen, um den Schutz der Haftungsbeschränkung weiterhin beanspruchen zu können.[970]

Welchen Schwierigkeiten sich ein Rechtsinhaber in einem Prozess gegenüber sehen kann, diese hohen Hürden des *red-flags*-Tests zu nehmen, zeigte anschaulich das Verfahren *Perfect 10, Inc. v. CCBill LLC*.[971] Dabei ging es um die Haftung eines ISPs, der für die Betreiber von Webseiten Zahlungen der Nutzer über das Internet abwickelte. Auf einigen der vom Beklagten betreuten Webseiten wurden die Urheberrechte an Fotografien des klagenden Rechtsinhabers verletzt. Teilweise trugen diese Webseiten so bezeichnende Titel wie „illegal.net" und „stolencele-

967 H.R. Rep. 105-551 (II), S. 57.

968 H.R. Rep. 105-551 (II), S. 57-58: *„For instance, the copyright owner could show that the provider was aware of facts from which infringing activity was apparent if the copyright owner could prove that the location was clearly ... a „pirate" site of the type described below, where sound recordings, software, movies or books were available for unauthorized downloading, public performance, or public display. ... The intended objective of this standard is to exclude from the safe harbor sophisticated „pirate" directories ... Such pirate directories refer Internet users to sites that are obviously infringing because they typically use words such as „pirate", „bootleg", or slang terms in their URL and header information to make their illegal purpose obvious, in the first place, to the pirate directories as well as other Internet users."*

969 *Darrow/Ferrera*, 6 Nw. J. Tech. & Intell. Prop. 1, 21 (2007).

970 H.R. Rep. 105-551 (II), S. 58: *„In this way, the ‚red flag' test in this new Section 512(d) strikes the right balance. The common-sense result of this ‚red flag' test is that on-line editors and catalogers would not be required to make discriminating judgements about potential copyright infringement. If, however, an Internet site is obviously pirate, then seeing it may be all that is needed for the service provider to encounter a ‚red flag'."*

971 *Perfect 10 v. CCBill*, 488 F.3 d 1102 (9th Cir. 2007).

britypics.com“. Dennoch verneinte der Ninth Circuit das Vorliegen von *red flags* im Sinne von § 512(c)(1)(A), da diese Bezeichnungen eher als Hinweis auf die „schlüpfrige“ Natur der auf diesen Seiten angebotenen Fotografien – die, wie auch die Bilder des Beklagten, Abbildungen pornographischen Inhalts enthielten – verstanden werden könnten denn auf den Umstand, dass es sich hierbei um urheberrechtswidrige Raubkopien handelte.[972] Auf der Grundlage dieser Entscheidung kam weiterhin der District Court in *UMG Recordings, Inc. v. Veoh Networks, Inc.* zu dem Ergebnis, dass das Vorliegen von *red flags* im Sinne von § 512(c)(1)(A) immer dann zu verneinen ist, wenn die Rechtswidrigkeit des betroffenen Materials erst nach einer näheren Untersuchung der bekannt gewordenen Umstände festgestellt werden kann.[973]

(3) Unverzügliches Tätigwerden nach Kenntniserlangung

Der Schutz der Safe-Harbor-Regelung gemäß § 512(c)(1)(A)(iii) entfällt selbst bei Vorliegen von positiver Kenntnis oder Umstandskenntnis seitens des Rechtsinhabers erst dann, wenn der ISP, nachdem er solche Kenntnis erlangt hat, nicht unverzüglich Maßnahmen zur Beseitigung des rechtswidrigen Materials ergreift. Mit dieser Regelung sollte verhindert werden, dass „redliche“ ISPs, die sich freiwillig darum bemühen, rechtswidriges Material aufzufinden und zu beseitigen, den Schutz der Haftungsbeschränkung allein deswegen verlieren, weil sie infolge ihrer freiwilligen Bemühungen Kenntnis von Urheberrechtsverletzungen erhalten.[974] Der Schutz der Haftungsbeschränkung erlischt somit selbst bei Kenntnis von einer Urheberrechtsverletzung erst dann, wenn der ISP trotz seiner Kenntnis nicht unverzüglich Maßnahmen ergreift, um die Rechtsverletzung zu beseitigen. Mit Kenntniserlangung unterliegt der ISP somit einer Pflicht zum Handeln, wenn er weiterhin den Schutz der Safe-Harbor-Regelung für sich beanspruchen will.[975] Im Hinblick auf die Unverzüglichkeit der Beseitigung legte sich der Gesetzgeber auf keinen bestimmten Zeitraum fest. Die Anforderungen an die Schnelligkeit der Re-

972 488 F.3 d 1102, 1114: *„Because CWIE and CCBill provides services to „illegal.net“ and „stolencelebritypics.com“, Perfect 10 argues that they must have been aware of apparent infringing activity. We disagree. When a website traffics in pictures that are titillating by nature, describing photographs as „illegal“ or „stolen“ may be an attempt to increase their salacious appeal, rather than an admission that the photographs are actually illegal or stolen. We do not place the burden of determining whether photographs are actually illegal on a service provider.“*

973 2009 U.S. Dist. LEXIS 86932, *24 (C.D. Cal. 2009): *“*CCBill *teaches that if investigation of facts and circumstances is required to identify material as infringing, then those facts and circumstances are not “red flags”.”*

974 *Darrow/Ferrera*, 6 Nw. J. Tech. & Intell. Prop. 1, 22 (2007).

975 *ALS Scan Inc. v. RemarQ Communities Inc.*, 239 F.3 d 619, 625 (4th Cir. 2001); *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.04[A][2], 12B – 54.

aktion eines ISPs sind somit grundsätzlich einzelfallabhängig für den konkreten Sachverhalt zu ermitteln, wobei insbesondere die jeweils gegebenen technischen Parameter eine entscheidende Rolle spielen.[976]

bb. Differenzierung der subjektiven Voraussetzungen gemäß § 512(c)(1)(A) von den Voraussetzungen des *contributory infringement*

Die subjektiven Voraussetzungen gemäß § 512(c)(1)(A) wurden in Anlehnung an die Tatbestandsvoraussetzungen des Rechtsinstituts des *contributory infringement*[977] entwickelt und sind teilweise mit diesen identisch.[978] Es stellt sich daher die Frage, ob die Safe-Harbor-Regelung gemäß § 512(c) auf einen ISP Anwendung finden kann, der als *contributory infringer* für die Urheberrechtsverletzung eines Nutzers seines Internetdienstes haftet und damit notwendigerweise die subjektiven Voraussetzungen dieses Rechtsinstituts erfüllt.[979]

Für die Haftung als *contributory infringer* reicht die positive Kenntnis von dem rechtswidrigen Material oder der rechtswidrigen Handlung an sich aus, d.h. die Kenntnis der Rechtswidrigkeit ist insoweit nicht erforderlich. Hingegen ist nach der ersten Tatbestandsalternative gemäß § 512(c)(1)(A)(i) für den Verlust der Haftungsbeschränkung erforderlich, dass seitens des ISPs positive Kenntnis gerade auch der Rechtswidrigkeit des in seinem System befindlichen Materials bzw. der darin stattfindenden Aktivität des Nutzers besteht. Dies bedeutet, dass ein ISP, der auf der Ebene der Haftungsbegründung als *contributory infringer* wegen positiver Kenntnis haftet, dennoch in den Genuss der Haftungsbeschränkung kommen kann, wenn seine Kenntnis sich nicht auch auf die Rechtswidrigkeit, sondern nur auf die Handlung oder das Material an sich bezieht. Darüber hinaus greift die Haftungsbeschränkung gemäß § 512(c)(1)(A)(iii) trotz positiver Kenntnis auch von der Rechtswidrigkeit des Materials oder der Handlung auch dann ein, wenn der ISP nach Kenntniserlangung umgehend Maßnahmen zur Beseitigung des rechtswidrigen Materials ergreift.

Fraglich ist weiterhin, inwieweit die Kenntnisalternative der *constructive knowledge* des Rechtsinstituts des *contributory infringement* und der Umstandskenntnis gemäß § 512(c) deckungsgleich sind. Ebenso wie in Bezug auf das Erfordernis der positiven Kenntnis gilt auch hier, dass sich die Umstandskenntnis im Rahmen von § 512(c) auf die Rechtswidrigkeit eines Verhaltens oder eines Inhalts beziehen muss. Weiterhin hat die Analyse des für die Prüfung der Umstandskenntnis maß-

976 H.R. Rep. 105-551 (II), S. 53-54.
977 Vgl. 8. Kapitel, Teil B.II.2.
978 *Goldstein*, Copyright, 2005, § 6.3.1, 6:33.
979 Vgl. hierzu die ausführliche Darstellung von *Reese*, 32 Colum. J.L. & Arts 427 (2009); *ders*., 34 Sw. U. L. Rev. 287, 288 (2004).

geblichen *red-flag*-Tests gezeigt, dass an das Vorliegen von Umständen, die die Rechtswidrigkeit eines Materials oder einer Handlung indizieren, sehr hohe Anforderungen gestellt werden. Denn die Prüfung muss ergeben, dass vom subjektiven Standpunkt des ISPs aus gesehen diesem Umstände bewusst waren, die objektiv als *red flags*, d.h. als Tatsachen, die ein rechtswidriges Verhalten offensichtlich indizieren, zu qualifizieren sind. Damit sind die Anforderungen an das Vorliegen von *red flags* jedoch wesentlich höher als diejenigen betreffend das Vorliegen von *constructive knowledge*, wofür nach Auffassung mancher Gerichte bereits ausreicht, dass der ISP sich vor der Kenntnis von Rechtsverletzungen bewusst verschließt.[980] Dies bedeutet jedoch, dass das Vorliegen von *constructive knowlege* seitens des ISPs nicht automatisch das Vorliegen von *red flags* indiziert.[981] Zudem gilt auch hier, dass der ISP den Schutz der Safe-Harbor-Regelung gemäß § 512(c) auch trotz des Vorliegens von Umstandskenntnis beanspruchen kann, wenn er das rechtswidrige Material nach Erlangung des Bewusstseins von *red flags* unverzüglich entfernt.

Im Ergebnis bleibt somit festzuhalten, dass zwar Überschneidungen zwischen den Voraussetzungen der mittelbaren Haftung und den subjektiven Ausschlusskriterien der Safe-Harbor-Regelung gemäß § 512(c) bestehen, diese jedoch keinesfalls identisch sind. Aus der Tatsache, dass ein ISP wegen positiver Kenntnis oder *constructive knowledge* von einer Rechtsverletzung als *contributory infringer* haftet, lässt sich somit nicht automatisch auf die Unanwendbarkeit der Haftungsbeschränkung schließen.[982]

cc. Bewertung: Auswirkungen von Content-Identification-Technologien auf die subjektiven Voraussetzungen gemäß § 512(c)(1)(A)

Nachfolgend wird das Vorliegen der subjektiven Ausschlusskriterien in Bezug auf Web 2.0-Dienste geprüft und inwieweit sich die Verfügbarkeit von Content-Identification-Technologien hierauf auswirkt.

Wie bereits mehrfach dargestellt wurde, ist im Falle eines Web 2.0-Dienstes im Regelfall nicht davon auszugehen, dass dieser positive Kenntnis von einzelnen, innerhalb seines Internetdienstes begangenen Rechtsverletzungen hat. Denn zum einen erfolgt der Prozess des Hochladens von Inhalten automatisiert und wird allein durch den jeweiligen Nutzer gesteuert. Dies bedeutet, dass die Einstellung von Inhalten und damit die Begehung von Rechtsverletzungen durch das Hochladen von Kopien von urheberrechtlich geschützten Multimediawerken typischerweise

980 Vgl. 8. Kapitel, B.II.2.b.(bb)(5).
981 *Reese*, 34 Sw. U. L. Rev. 287, 300 (2004).
982 So auch *Reese*, 32 Colum. J.L. & Arts 427, 436 (2009).

ohne Ein- oder Mitwirkung des ISPs bzw. seiner Mitarbeiter erfolgt. Zum anderen ist es bereits aufgrund der schieren Datenmengen, die tagtäglich auf einen Web 2.0-Dienst eingestellt werden, dem ISP nicht möglich, alle Inhalte einzeln zur Kenntnis zu nehmen.

Fraglich ist somit allein, ob auf den Umstand, dass ein ISP bewusst auf den Einsatz von Content-Identification-Technologien innerhalb seines Internetdienstes verzichtet, möglicherweise das Vorliegen von Umstandskenntnis gemäß § 512(c)(1)(A)(ii) gestützt werden kann. Gegen eine solche Ausdehnung des Begriffs der Umstandskenntnis wandte sich jedoch beispielsweise das Gericht in *Universal Recordings v. Veoh Networks* („Universal v. Veoh").[983] Hier setzte der beklagte Betreiber einer Videoplattform in seinem Internetdienst zwar eine Audio-Fingerprinting-Technologie des Anbieters Audible Magic ein, um rechtswidrige Inhalte auszufiltern.[984] Allerdings warfen die Rechtsinhaber dem Beklagten vor, eine solche Technologie nicht bereits zu einem früheren Zeitpunkt eingesetzt zu haben und argumentierten, dass der Beklagte wegen dieses verzögerten Einsatz einer Content-Identification-Technologie den Schutz der Safe-Harbor-Regelung nicht beanspruchen könne, da hieraus Umstandskenntnis in Form eines bewussten Sichverschließens vor der Kenntnis von Rechtsverletzungen seitens des Beklagten resultiere. Dem folgte das Gericht nicht und hielt zunächst ausdrücklich fest, dass es grundsätzlich keine Verpflichtung des Beklagten zum Einsatz einer solchen Technologie gebe. Daher könne es ihm auch nicht vorgeworfen werden, eine solche Technologie erst ab einem bestimmten Zeitpunkt eingesetzt zu haben. Hingegen schloss das Gericht aus dem Umstand, dass der Beklagte eine solche Technologie einsetzte, ohne hierzu verpflichtet zu sein, dass der Beklagte sich nach bestem Wissen und Gewissen darum bemühte, Urheberrechte im Rahmen seines Internetdienstes zu schützen, und damit den Schutz der Haftungsbeschränkung verdiente:

> „Universal also contends that Veoh avoided gaining knowledge of infringement by delaying implementation of the Audible Magic fingerprinting system until October 2007 even though it was available in early 2005, and by waiting nine months before filtering videos already on its system. ... Universal has not established that the DMCA imposes an obligation on a service provider to implement filtering technology from the copyright holder's preferred vendor or on the copyright holder's desired timeline. Moreover, it is undisputed that Veoh did take steps to implement filtering technology before it implemented the Audible Magic system that Universal prefers, by using „hash" filtering and by attempting to develop its own filtering software. Universal dismisses hash

983 *Universal Recordings, Inc. v. Veoh Networks Inc.,* 2009 U.S. Dist. LEXIS 86932 (C.D. Cal. 2009).

984 2009 U.S. Dist. LEXIS 86932, *8, 9.

filtering as „highly ineffectual", but that it proved deficient and that Veoh then turned to Audible Magic does not negate Veoh's showing of good faith efforts to avoid or limit storage of infringing content."[985]

Zudem scheitert eine solche Ausdehnung des Begriffs der Umstandskenntnis an dem auch im Rahmen von § 512(c) grundsätzlich geltenden Ausschluss von proaktiven Überwachungspflichten zu Lasten von ISPs. Denn würde man Umstandskenntnis allein auf die Tatsache stützen, dass ein ISP innerhalb seines Internetdienstes keine Content-Identification-Technologie einsetzt, würde man ihn hierdurch gleichsam zum Einsatz solcher Technologien verpflichten, wenn er sich weiterhin auf den Schutz der Haftungsbeschränkung berufen will. Damit würde er jedoch entgegen § 512(m) dazu verpflichtet, seinen Internetdienst zu überwachen und mit Hilfe von Content-Identification-Technologien auf das Vorhandensein von urheberrechtwidrigem Material zu durchsuchen. Da jedoch Content-Identification-Technologien keine STMs darstellen,[986] gilt der Ausschluss proaktiver Überwachungspflichten weiterhin ohne jede Einschränkung und dürfen ISPs zum Einsatz solcher Technologien nicht verpflichtet werden.

Die Verfügbarkeit von Content-Identification-Technologien hat somit keine Auswirkungen auf die Beurteilung des Vorliegens der subjektiven Voraussetzungen gemäß § 512(c)(1)(A). Insbesondere kann das Vorliegen von Umstandskenntnis seitens eines ISPs nicht aufgrund der Tatsache konstruiert werden, dass dieser im Rahmen seines Internetdienstes bewusst auf den Einsatz von Content-Identification-Technologien verzichtet.

e. Ausschlusskriterium gemäß 17 U.S.C. § 512(c)(1)(B)

Die Anwendbarkeit der Haftungsbeschränkung gemäß § 512(c) scheidet weiterhin aus, wenn der ISP die rechtliche und die tatsächliche Möglichkeit hat, das rechtswidrige Verhalten seiner Nutzer zu kontrollieren und ihm aus dem Verhalten ein unmittelbarer wirtschaftlicher Vorteil erwächst.[987]

985 2009 U.S. Dist. LEXIS 86932, *35.
986 Vgl. 8. Kapitel, Teil B.III.4.a.cc.
987 § 512(c)(1)(B): *„A service provider shall not be liable ... if the service provider ... does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity... ."*

aa. Rechtliche und tatsächliche Kontrollmöglichkeit

Die Gesetzesmaterialen geben keinerlei Hinweise auf die Auslegung der Voraussetzung der tatsächlichen Kontrollmöglichkeit in Bezug auf rechtswidriges Verhalten (nachfolgend „tatsächliche Beherrschungsmöglichkeit") im Rahmen von § 512(c).[988] Da zu dieser Frage bislang auch noch nicht viel *case law* ergangen ist, sind bisher nur einige wenige Aspekte dieser Tatbestandsvoraussetzung in Ansätzen geklärt.

(1) Das Verhältnis von § 512(c)(1)(B) zu den Anforderungen des Verfahrens gemäß § 512(c)(3)

Aus dem bisher ergangenen *case law* geht hervor, dass die technischen Mittel, über die der ISP verfügen muss, um urheberrechtswidriges Material im Einklang mit dem Notice&Takedown-Verfahren gemäß § 512(c)(3)[989] aus seinem Internetdienst zu entfernen, nicht zur Begründung der notwendigen tatsächlichen Kontrollmöglichkeit im Sinne von § 512(c)(1)(B) ausreichen. Hierüber besteht unter den Gerichten weitgehende Einigkeit.[990] Zwar kann ein ISP durch solche Mittel zur Beseitigung oder Sperrung von angeblich urheberrechtswidrigem Material die Nutzung seines Internetdienstes bis zu einem gewissen Grad steuern. Würden jedoch diese Eingriffsmöglichkeiten für sich genommen ausreichen, um die Voraussetzung der tatsächlichen Kontrolle zu erfüllen und damit die Anwendbarkeit der Haftungsbeschränkung gemäß § 512(c)(1)(B) auszuschließen, würde dies zu einer unzumutbaren Zwickmühle zu Lasten der ISPs führen.[991] Denn die Einhaltung des Verfahrens gemäß § 512(c)(3) ist ebenfalls eine Voraussetzung der Anwendbarkeit

988 Vgl. H.R. Rep. (II), S. 54. In Bezug auf § 512(c)(1)(B) werden nur einige Hinweise zur Auslegung des "financial benefit criterion" gegeben, siehe hierzu nachfolgendes Kapitel.

989 Vgl. 8. Kapitel, Teil B.III.4.f. Um den Anforderungen des Notice&Takedown-Verfahrens erfüllen zu können, muss der ISP insbesondere rechtswidriges Material aus seinem Internetdienst entfernen bzw. den Zugang hierzu sperren können.

990 *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2 d 1082, 1094 (C.D. Cal. 2001); Corbis *Corporation v. Amazon.com, Inc.*, 351 F. Supp. 2 d 1090, 1110 (W.D. Wash. 2004); s.a. *Perfect 10, Inc.v. Cybernet Ventures, Inc.*, 213 F. Supp. 2 d 1146, 1181 (C.D. Cal. 2002); *Ellison v. Robertson*, 189 F. Supp. 2 d 1051 (C.D. Cal. 2002); *UMG Recordings, Inc. v. Veoh Networks Inc.*, 2009 U.S. Dist. LEXIS 86932, **37-38 (C.D. Cal. 2009).

991 *Hendrickson v. eBay, Inc*., 165 F. Supp. 2 d 1082, 1093-94 (C.D. Cal. 2001): *„Congress could not have intended for courts to hold that a service provider loses immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically required by the DMCA."*; *Ellison v. Robertson*, 189 F. Supp. 2 d 1051, 1061 (C.D. Cal. 2001): *"It is conceivable that Congress intended that ISPs which receive a financial benefit directly attributable to the infringing activity would not, under any circumstances, be able to qualify for the subsection (c) safe harbour. ... The Court does not accept that Congress would express its desire to do so by creating a confusing, self-contradictory catch-22 situation that pits 512(c)(1)(B) and 512(1)(C) directly at odds with one another... ."*

der Haftungsbeschränkung gemäß § 512(c). Würde somit ein ISP wegen des Ausschlusskriteriums gemäß § 512(c)(1)(B) darauf verzichten, innerhalb seines Internetdienstes die technischen Voraussetzungen zur Beseitigung von rechtswidrigem Material gemäß § 512(c)(3) zu schaffen, könnte er dadurch das Notice&Takedown-Verfahren nicht mehr einhalten und verlöre dann aus diesem Grund den Anspruch auf die Haftungsbeschränkung. Daher fordern die Gerichte, dass zur Erfüllung der Voraussetzung der faktischen Beherrschungsmöglichkeit seitens des ISPs ein „Mehr" an Einfluss in Bezug auf das rechtswidrige Verhalten des Nutzers gegeben sein muss als die Möglichkeit, rechtswidriges Material *nach* dessen Speicherung innerhalb des Systems des ISPs entsprechend den Anforderungen des Notice&Takedown-Verfahrens zu entfernen oder zu sperren.[992]

(2) Das rechtsverletzende Verhalten als Bezugspunkt der tatsächlichen Kontrollmöglichkeit

Maßgeblich für das Vorliegen der tatsächlichen Kontrollmöglichkeit ist weiterhin, dass der ISP nicht nur *die innerhalb seines Systems oder Netzwerks vorhandenen Inhalte*, sondern darüber hinaus gerade auch die *rechtsverletzenden Aktivitäten* der Nutzer kontrollieren kann.

Dies geht insbesondere auch aus der Entscheidung *IO v. Veoh*[993] hervor. Der in diesem Verfahren beklagte ISP führte innerhalb seines Internetdienstes gelegentliche „spot checks" durch um zu überprüfen, ob die Nutzer die Vorgaben seiner Nutzungsbedingungen betreffend die inhaltliche Zulässigkeit von Videomaterial einhielten. Im Falle eines Verstoßes gegen die Nutzungsbedingungen entfernte der ISP das rechtswidrige Material und beendete die Nutzungsberechtigung des betreffenden Nutzers.[994] Vor diesem Hintergrund argumentierten die klagenden Rechtsinhaber, dass der ISP aufgrund dieser *spot checks* über die gemäß § 512(c)(1)(B) erforderliche Kontrollmöglichkeit verfügen würde. Das Gericht vertrat hingegen die Auffassung, dass eine faktische Beherrschungsmöglichkeit im Sinne der Haftungsbeschränkung nicht gegeben sei, da hierfür nicht ausreiche, dass der Beklagte die Möglichkeit habe, das von ihm angebotene *System* oder *Netzwerk* zu kontrollieren. Vielmehr sei erforderlich, dass er das konkrete urheberrechtswidrige

992 *Ellison v. Robertson*, 189 F. Supp. 2 d 1051, 1061 (C.D. Cal. 2001); *Perfect 10, Inc. v. Cybernet Ventures*, Inc., 213 F. Supp. 2 d 1146, 1173-74, 1181 (C.D. Cal. 2002).
993 2008 U.S. Dist. LEXIS 65915, *46 ff. (N.D. Cal. 2008).
994 2008 U.S. Dist. LEXIS 65915, *46-47.

Verhalten des Nutzers beherrschen könne.[995] Dies ergebe sich daraus, dass nach der Formulierung in § 512(c)(1) das Gesetz für die Anwendbarkeit von § 512(c) von vornherein voraussetze, dass der ISP sein System oder Netzwerk kontrollieren könne. Wenn jedoch das Gesetz die Kontrollmöglichkeit des Systems oder Netzwerks des ISPs als selbstverständlich voraussetzt, kann dies nicht gleichzeitig einen speziellen Umstand darstellen, der zum Ausschluss der Anwendbarkeit der Haftungsbeschränkung führt. Weiterhin ginge aus dem Wortlaut von § 512(c)(1)(B) hervor, dass sich der wirtschaftliche Vorteil und die Kontrollmöglichkeit des ISP unmittelbar auf das rechtswidrige Verhalten beziehen müssten. Über eine solche Kontrollmöglichkeit verfügte der beklagte ISP jedoch nicht, da er lediglich die Nutzerkonten von *repeat infringers* beenden sowie rechtswidriges Material, von dem er im Rahmen des Verfahrens gemäß § 512(c)(3) informiert worden war, aus dem Internetdienst entfernen konnte, nicht jedoch auf das Nutzerverhalten selbst einwirken konnte.

(3) Keine Verpflichtung zur Ausschöpfung von theoretisch möglichen Kontrollmöglichkeiten

Weiterhin geht aus der Entscheidung *Universal v. Veoh* hervor, dass zur Erfüllung des Kriteriums der tatsächlichen Kontrollmöglichkeit nicht die theoretische Möglichkeit ausreicht, dass ein ISP innerhalb seines Dienstes zusätzliche Technologien wie beispielsweise eine Content-Identification-Technologie einsetzen könnte, um das Verhalten der Nutzer besser zu kontrollieren.[996] Begründet wurde dies damit, dass unter diesem Ansatz ISPs faktisch zum Einsatz solcher Technologien verpflichtet würden. Damit würde jedoch einer der maßgeblichen Grundsätze, auf denen die Safe-Harbor-Regelung beruht, nämlich der Ausschluss proaktiver Überwachungspflichten gemäß § 512(m), untergraben:

> „Veoh's „right and ability" to implement filtering software, standing alone or even along with Veoh's ability to control user's access, also cannot be the basis for concluding that Veoh is not eligible for section 512(c) safe harbor. Section 512(m) provides that „[n]othing in this section shall be construed to condition the applicability of subsections (a) through (d) on ... a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a STM complying with the provisions of

995 2008 U.S. Dist. LEXIS 65915, *47: *„... the plain language of section 512(c) indicates that the pertinent inquiry is not whether Veoh has the right and ability to control its* system*, but rather, whether it has the right and ability to control the* infringing activity." (Hervorhebung durch die Verfasserin).

996 2009 U.S. Dist. LEXIS 86932, *39 (C.D. Cal. 2009.).

subsection (i)". If courts were to find that the availability of superior filtering systems or the availability to search for potentially infringing files establishes – without more – that a service provider has „the right and ablitity to control" infringement, that would effectively require service providers to adopt specific filtering technology and perform regular searches. That, in turn, would impermissibly condition the applicability of section 512(c) on a service provider monitoring its service or affirmatively seeking facts indicating infringing activity".[997]

Ebenso weigerte sich der District Court in *IO v. Veoh* zu berücksichtigen, dass der ISP theoretisch sämtliche von den Nutzern auf seinen Internetdienst hochgeladenen Videodateien auf ihre Herkunft und Rechtmäßigkeit hätte überprüfen und zur Erfüllung dieser Aufgabe gegebenenfalls zusätzliches Personal einstellen bzw. den Umfang seines Dienstes auf ein kontrollierbares Maß begrenzen hätte können. Denn bei der Prüfung der Frage, ob ein ISP es versäumt hat, eine ihm offenstehende tatsächliche Kontrollmöglichkeit in Bezug auf rechtswidriges Verhalten auszuüben, dürfe nicht dessen Geschäftsmodell in Gänze in Frage gestellt werden.[998] Ausreichend sei vielmehr, dass ein ISP die ihm unter den gegebenen Umständen zur Verfügung stehenden Kontrollmöglichkeiten vollumfänglich ausschöpfe. Dies habe der Beklagte ISP jedoch getan[999] und darüber hinaus zusätzlich eine Filtertechnologie eingesetzt, durch die das wiederholte Einstellen von bereits als rechtswidrig identifiziertem, identischem Material verhindert werden sollte.[1000]

Darüber hinaus geht aus der Gesetzesbegründung hervor, dass Maßnahmen, die ein ISP freiwillig zum Zwecke der Überwachung seines Internetdienstes ergreift, grundsätzlich nicht zu Lasten des ISPs gehen dürfen, d.h. für sich genommen nicht zum Verlust der Haftungsbeschränkung führen dürfen.[1001]

997 2009 U.S. Dist. LEXIS 86932, *38, 39.

998 2008 U.S. Dist. LEXIS 65915, *57: *"Declining to change business operations is not the same as declining to exercise a right and ability to control infringing activity."*

999 2008 U.S. Dist. LEXIS 65915, *55-56.

1000 2008 U.S. Dist. LEXIS 65915, *56; *Sloane/McMahon*, CRi 2009, 6.

1001 H.R. Conf. Rep. 105-796, S. 73: *„This legislation is not intended to discourage the service provider from monitoring its service for infringing material. Courts should not conclude that the service provider loses eligibility for limitations on liability under section 512 solely because it engaged in a monitoring program."* Nach *Reese*, 34 Sw. U. L. Rev. 287, 302 (2004), darf deswegen die Kenntnis von einem Rechtsverstoß, die ein ISP nur aufgrund von freiwillig durchgeführten Überwachungsmaßnahmen erhalten hat, im Rahmen von § 512(c) unter keinen Umständen zum Nachteil des ISPs gereichen.

bb. Unmittelbarer wirtschaftlicher Vorteil

Weiterhin ist im Rahmen von § 512(c)(1)(B) erforderlich, dass dem ISP aus dem rechtswidrigen Verhalten des Nutzers, das er entsprechend den zuvor dargestellten Grundsätzen kontrollieren kann, ein unmittelbarer wirtschaftlicher Vorteil erwächst. Ebenso wie im Zusammenhang mit der Voraussetzung der tatsächlichen Beherrschungsmöglichkeit ist zum gegenwärtigen Zeitpunkt mangels einschlägigem *case law* noch weitgehend unklar, was unter diesem Erfordernis im Einzelnen zu verstehen ist.[1002]

Aus der Gesetzesbegründung geht hervor, dass die Gerichte bei der Auslegung dieser Voraussetzung einen „common-sense, fact-based approach" walten und sich nicht von rein formalistischen Aspekten leiten lassen sollen.[1003] Das Vorliegen dieser Voraussetzung ist demnach zu verneinen, wenn die Gesamtbetrachtung ergibt, dass der ISP dem Grunde nach ein „seriöses Geschäft" betreibt.[1004] Davon ist beispielsweise dann auszugehen, wenn alle Nutzer des Internetdienstes unabhängig davon, ob sie den Internetdienst des ISPs für legale oder illegale Zwecke nutzen, hierfür die gleiche Gegenleistung erbringen. Weiterhin spricht für ein seriöses Geschäft, dass sich die an den ISP zu zahlenden Entgelte anhand „neutraler" Kriterien wie beispielsweise der übermittelten Datenmenge oder der Zeitdauer der Nutzung, nicht jedoch nach der Art des übermittelten Inhalts berechnen.

Weiterhin sollen ISPs grundsätzlich nicht für die Entscheidung für ein bestimmtes Vergütungs- und Geschäftsmodell „bestraft" werden.[1005] Zur Bejahung der Voraussetzung des *direct financial benefit* darf das vom ISP praktizierte Geschäftsmodell daher grundsätzlich nur herangezogen werden, wenn sich hieraus ein offensichtliches Interesse des ISPs an den urheberrechtswidrigen Aktivitäten der Nutzer ergibt. Dies ist beispielsweise dann der Fall, wenn der Wert eines Internet-

1002 *Reese*, 32 Colum. J.L. & Arts 427, 441 (2009).

1003 H.R. Rep. (II), S. 54; *Goldstein*, Copyright, 2005, § 6.3.1, 6:34-1. Diese gesetzgeberische Vorgabe entspricht dem von *Ginsburg*, 50 Ariz. L. Rev. 577, 579 (2008) formulierten Postulat, wonach die Haftung eines Technologieanbietern von der haftungsrechtlichen "Neutralität" von dessen Geschäftsmodell abhängen soll: *"… Or can we have it both ways, fostering both authorship and technological innovation? To reach that happy medium, we need to ensure the "neutrality" of the technology as applied in a given business setting. If the entrepreneur is not neutral, and is in fact building its business at the expense of authors and right owners, it should not matter how anodyne in the abstract the technology may be."*

1004 H.R. Rep. 105-551 (II), S. 54: "*In determining whether the financial benefit criterion is satisfied, courts should take a common-sense, fact-based approach, not a formalistic one. In general, a service provider conducting a legitimate service would not be considered to receive a "financial benefit directly attributable to the infringing activity"…".*

1005 *Darrow/Ferrera*, 6 Nw. J. Tech. & Intell. Prop. 1, 25 (2007); *Kim*, 17 S. Cal. Interdis. L.J. 139, 162 (2007).

dienstes für die Nutzer gerade darin liegt, dass sie Zugang zu urheberrechtswidrigem Material erhalten.[1006]

Für die Auslegung der Voraussetzung des unmittelbaren wirtschaftlichen Vorteils im Rahmen der Safe-Harbor-Regelung bedeutet dies konkret, dass insbesondere das Verständnis des Begriffs „unmittelbar" („direct") enger am ursprünglichen Wortsinn orientiert werden muss. Somit dürften mittelbare und erst in Zukunft möglicherweise realisierbare wirtschaftliche Vorteile anders als im Rahmen der *vicarious liability* nicht zur Bejahung dieser Voraussetzung ausreichen.[1007] Eine in dieser Weise differenzierte Auslegung nahm auch das Gericht in *CoStar v. LoopNet* vor. Darin lehnte es das Gericht ab, das Vorliegen dieser Voraussetzung in Anlehnung an *Fonovisa*[1008] allein darauf zu stützen, dass sich durch die Rechtsverletzungen der Nutzer die Attraktivität des Dienstes des Beklagten erhöhen würde. Denn nach dem ausdrücklichen Wortlaut des Gesetzes müsse der wirtschaftliche Vorteil *unmittelbar* mit der Rechtsverletzung verbunden sein und reichten daher lediglich *mittelbare* Vorteile nicht aus.[1009] Damit sprach sich das Gericht jedoch implizit gegen eine undifferenzierte Heranziehung des *case law* zur *vicarious liability* im Zusammenhang mit der Safe-Harbor-Regelung aus.[1010]

cc. Differenzierung der Anforderungen gem. § 512(c)(1)(B) von den Voraussetzungen der vicarious liability

Die Voraussetzungen für den Ausschluss der Anwendbarkeit der Haftungsbeschränkung gemäß § 512(c)(1)(B) sind gleichlautend mit den Voraussetzungen der *vicarious liability,*[1011] auf deren Grundlage sie entwickelt wurden.[1012] Es stellt sich somit – ähnlich wie im Rahmen von § 512(c)(1)(A) in Bezug auf das Rechtsinstitut des *contributory infringement*[1013] – die Frage, ob und inwieweit ein ISP, der dem Grunde nach als *vicarious infringer* haftet, angesichts der gleichlautenden Voraussetzungen des Ausschlusskriteriums gemäß § 512(c)(1)(B) noch durch § 512(c) vor einer Haftung geschützt werden kann.[1014]

1006 H.R. Rep. 105-551 (II), S. 54: *"It [the financial benefit criterion] would however, include any such fees where the value of the service lies in providing access to infringing material."*
1007 *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.04[A][2], 12B – 55, Fn. 30.1; *Ott*, GRUR Int. 2008, 563, 567; *Holznagel*, GRUR Int. 2008, 971, 975.
1008 Vgl. 8. Kapitel, Teil B.II.3.b.(bb)(1).
1009 *CoStar Group, Inc. v. LoopNet, Inc.*, 164 F. Supp. 2 d 688, 705 (D. Md. 2001).
1010 *CoStar Group, Inc. v. LoopNet, Inc.*, 164 F. Supp. 2 d 688, 704-05; *Breen*, YouTube or YouLose?, 2007, S. 16.
1011 Vgl. 8. Kapitel, Teil B.II.3.
1012 *IO Group, Inc. v. Veoh Networks, Inc.*, 2008 U.S. Dist. LEXIS 65915, *45; *Goldstein*, Copyright, 2005, § 6.3.1, 6:34.
1013 Vgl. 8. Kapitel, Teil B.II.2.
1014 Vgl. hierzu die ausführliche Darstellung bei *Reese*, 32 Colum. J.L. & Arts 427 (2009).

Aus der Tatsache der Identität der Ausschlusskriterien gemäß § 512(c)(1)(B) und der Tatbestandsvoraussetzungen des Rechtsinstituts der *vicarious liability* wird teilweise geschlossen, dass den insoweit verwendeten Begrifflichkeiten dieselbe inhaltliche Bedeutung zukommt.[1015] Dies begründete der Ninth Circuit in *Perfect 10 v. CCBill* damit, dass die sich aus dem *common law* ergebenden Vorgaben in Bezug auf die Auslegung eines Rechtsbegriffs auch für die Auslegung eines identischen Begriffs in einem anderen Kontext maßgeblich sind, wenn keine Anhaltspunkte dafür vorliegen, dass eine differenzierende Auslegung geboten ist.[1016] Solche Anhaltspunkte für eine gebotene abweichende Auslegung sah das Gericht im Zusammenhang mit § 512(c)(1)(B) nicht. Ebenso ging das Gericht in *Aimster* von einem Gleichlauf der inhaltlichen Bedeutung dieser Begriffe aus, was daraus hervorgeht, dass die Anwendungsvoraussetzungen gemäß § 512(c)(1)(B) keiner separaten Prüfung unterzogen wurden, sondern insoweit lediglich auf die Ausführungen zu den Voraussetzungen der *vicarious liability* verwiesen wurde.[1017]

Ein solcher Gleichlauf der Auslegung würde im Ergebnis jedoch bedeuten, dass ein ISP, der für die Urheberrechtsverletzungen der Nutzer im Rahmen seines Internetdienstes als *vicarious infringer* haftet, nie in den Genuss der Haftungsbeschränkung gemäß § 512(c) kommen könnte.[1018] Dieses Ergebnis widerspricht jedoch der gesetzgeberischen Intention, wonach durch die Safe-Harbor-Regelung neben den Folgen der Primär- grundsätzlich auch diejenigen der Sekundärhaftung beschränkt werden sollten,[1019] wozu auch das Rechtsinstitut der *vicarious liability* zählt.[1020] Insoweit ist auch zu berücksichtigen, dass die *primary liability* eines

1015 Vgl. beispielsweise *Perfect 10 v. CCBill*, 488 F.3 d 1102, 1117 (9th Circ. 2007): *„…'direct financial benefit' should be interpreted consistent with the similarly-worded common law standard for vicarious copyright liability"*; ebenso *Ginsburg*, 50 Ariz. L. Rev. 577, 601 (2008).

1016 488 F.3 d 1102, 1117: *„Based on the well-established rule of construction that where Congress uses terms that have accumulated settled meaning under common law, a court must infer, unless the statute otherwise dictates, that Congress means to incorporate the established meaning of these terms, we hold that ‚direct financial benefit' should be interpreted consistent with the similarly-worded common law standard for vicarious copyright liability. Thus, the relevant inquiry is whether the infringing activity constitutes a draw for subscribers, not just an added benefit."*; s.a. Anm. *Band*, CRi 2007, 122, 123 f.

1017 *In re Aimster Copyright Litigation*, 252 F. Supp. 2 d 634, 661 (N.D. Ill. 2002); *Breen*, YouTube or YouLose?, 2007, S. 21.

1018 *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.04[A][2], 12B – 55.

1019 S. Rep. 105-190, S. 43: *„Subsection (c) limits the liability of qualifying service providers for claims of direct, vicarious and contributory infringement for storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider"*; H.R. 105-551 (II), S. 50; *Cloak*, 60 Vand. L. Rev. 1559, 1587-88 (2007); *Reese*, 34 Sw. U. L. Rev. 287, 288 (2004); a.A. *Ginsburg*, 50 Ariz. L. Rev. 577, 591 (2008), wonach die sog. „threshold requirements" gemäß § 512(c)(1)(A) und (B) sicherstellen sollen, dass nur ein „unschuldiger" Host-Provider, d.h. ein ISP, der gemäß der Grundsätze der *secondary liability* nicht haftet, in den Genuß der Haftungsbeschränkung kommt.

1020 Vgl. 8. Kapitel, Teil B.II.3.

ISPs oftmals bereits nach den Grundsätzen von *Netcom* ausscheidet,[1021] so dass die Safe-Harbor-Regelung für die Primärhaftung von ISPs ohnehin nur eine eingeschränkte Rolle spielt. Wäre darüber hinaus die Anwendbarkeit von § 512(c) auf eines der beiden Rechtsinstitute der Sekundärhaftung ausgeschlossen, verbliebe kaum mehr ein relevanter Anwendungsbereich für diese Haftungsbeschränkung.[1022] Der hinter den Safe-Harbor-Regelungen stehende Zweck der Schaffung von Rechtssicherheit für ISPs kann somit nur durch eine differenzierte Auslegung der Begrifflichkeiten von § 512(c)(1)(B) erreicht werden.

Auch hat die Analyse der einzelnen Voraussetzungen des Ausschlusskriteriums gemäß § 512(c)(1)(B) gezeigt, dass sowohl aus der Gesetzesbegründung als auch aus dem bisher ergangenen *case law* hervorgeht, dass unter bestimmten Aspekten eine differenzierte Auslegung aufgrund des unterschiedlichen Kontexts, in dem diese Begriffe verwendet werden, unumgänglich ist. So dürfen beispielsweise die technischen Funktionen, die der Erfüllung der Anforderungen des Notice&Takedown-Verfahrens dienen, sowie freiwillig implementierte Maßnahmen des ISPs zur Verbesserung der Kontrolle über das Nutzerverhalten bei der Prüfung der Voraussetzung der tatsächlichen Kontrollmöglichkeit des ISPs im Kontext der Safe-Harbor-Regelung nicht berücksichtigt werden. Darüber hinaus sind höhere Anforderungen an die Voraussetzung des unmittelbaren rechtlichen Vorteils zu stellen, vor allem hinsichtlich der Unmittelbarkeit des aus dem unmittelbar rechtswidrigen Verhalten resultierenden wirtschaftlichen Vorteils zugunsten des ISPs.

Festzuhalten bleibt, dass sich auch das Ausschlusskriterium gemäß § 512(c)(1)(B) trotz der bestehenden begrifflichen Überschneidungen mit den Tatbestandsvoraussetzungen der *vicarious liability* von diesem Rechtsinstitut in seinen inhaltlichen Anforderungen unterscheidet. Dieses Ergebnis, wonach § 512(c) auch auf einen *vicarious infringer* Anwendung finden kann, entspricht der gesetzgeberischen Intention, durch die Safe-Harbor-Regelungen auch die Folgen der Sekundärhaftung zu beschränken.

dd. Bewertung: Auswirkungen von Content-Identification-Technologien auf das Ausschlusskriterium gemäß § 512(c)(1)(B)

Zu prüfen ist, ob das Ausschlusskriterium im Fall von Web 2.0-Diensten eingreift und inwieweit sich die Verfügbarkeit von Content-Identification-Technologien auf diese Beurteilung auswirkt.

1021 Vgl. 8. Kapitel, Teil B.I.2.
1022 Vgl. *Reese*, 32 Colum. J.L. & Arts 427 (2009).

(1) Rechtliche und tatsächliche Beherrschungsmöglichkeit

Wie bereits im Zusammenhang mit der *vicarious liability* dargelegt,[1023] können Web 2.0-Dienste, die keine Content-Identification-Technologien einsetzen, grundsätzlich keine tatsächliche Kontrolle über das rechtsverletzende Verhalten der Nutzer ausüben. An diesem Ergebnis ändert sich im Kontext der Safe-Harbor-Regelung insbesondere auch unter dem Aspekt nichts, dass einem ISP die Möglichkeit offen steht, Rechtsverletzungen im Rahmen des Notice&Takedown-Verfahrens nachträglich aus seinem Dienst zu entfernen. Denn wie gezeigt wurde, fordern die Gerichte, dass dem ISP ein über diese Möglichkeit hinausgehendes „Mehr" an Kontrolle zustehen muss. Auch darf das Vorliegen der Voraussetzung der tatsächlichen Kontrollmöglichkeit im Rahmen von § 512(c)(1)(B) nicht damit begründet werden, dass der ISP theoretisch die Möglichkeit hätte, eine Content-Identification-Technologien innerhalb seines Internetdienstes einzusetzen, wodurch er das notwendige Maß an Kontrolle erhalten würde. Denn dies würde dem Ausschluss proaktiver Überwachungspflichten gemäß § 512(m) zuwiderlaufen.[1024]

Fraglich ist jedoch, ob ebenso wie im Rahmen der *vicarious liability* auch im Zusammenhang mit § 512(c)(1)(B) davon auszugehen ist, dass ein ISP aufgrund des Einsatzes von Content-Identification-Technologien das notwendige Maß an Kontrolle betreffend das Nutzerverhalten besitzt. Dafür spricht, dass der ISP aufgrund dieses Umstandes über ein „Mehr" an Kontrolle über das urheberrechtswidrige Verhalten verfügt als die bloßen Einwirkungsmöglichkeiten zur Erfüllung der Anforderungen des Notice&Takedown-Verfahrens. Auch erhält der ISP durch den Einsatz einer solchen Technologie die Möglichkeit, unmittelbar auf das rechtsverletzende Verhalten selbst einzuwirken, anstatt „nur" bereits eingetretene Rechtsverletzungen nachträglich zu beseitigen.

Gegen die Berücksichtigung des Einsatzes einer Content-Identification-Technologie im Zusammenhang mit Voraussetzung der tatsächlichen Beherrschungsmöglichkeit spricht jedoch zum einen die gesetzgeberische Vorgabe, dass Maßnahmen, die ein ISP freiwillig ergreift, um innerhalb seines Internetdienstes Urheberrechte besser zu schützen, im Rahmen von § 512(c)(1)(B) grundsätzlich nicht zu seinen Lasten gehen dürfen und zum anderen, dass ISPs gemäß § 512(m) nicht zu einer proaktiven Überwachung ihres Internetdienstes verpflichtet werden dürfen. Da diese Vorgaben jedoch nur teilweise unmittelbar aus dem Gesetz hervorgehen, steht und fällt die Anwendbarkeit der Safe-Harbor-Regelung auf einen beklagten ISP damit, ob das befasste Gericht lediglich auf die begrifflich identischen Voraussetzungen der *vicarious liability* ergangene *case law* zurückgreift oder sich

1023 Vgl. 8. Kapitel, Teil B.II.3.c.(aa).
1024 2009 U.S. Dist. LEXIS 86932, *38, 39.

darüber hinaus vertieft mit dem Sinn und Zweck des Ausschlusskriteriums auseinandersetzt.

Den Mut zu einer solchermaßen differenzierten Auslegung der Voraussetzung der tatsächlichen Beherrschungsmöglichkeit im Rahmen von § 512(c) zeigte bisher beispielsweise das Gericht in *IO v. Veoh*[1025] Das Gericht lehnte es nach einer Gesamtbetrachtung des Verhaltens des beklagten Betreibers einer Videoplattform ab, hierin Umstände zu sehen, die zur einer Bejahung des Vorliegens der tatsächlichen Beherrschungsmöglichkeit im Sinne von § 512(c)(1)(B) und damit zum Ausschluss der Haftungsbeschränkung führen. Im Rahmen dieser Gesamtbetrachtung spielte auch die Tatsache, dass der Beklagte zur Identifizierung von Urheberrechtsverletzungen auch eine (Hash-)Filtertechnologie einsetzte, eine wichtige Rolle, die sich zugunsten des Beklagten auswirkte. Denn nach Auffassung des Gerichts zeigten die vom Beklagten freiwillig ergriffenen Maßnahmen, dass dieser seine Möglichkeiten zur Verhinderung von Urheberrechtsverletzungen nicht bewusst *nicht* vollumfänglich ausgeschöpft hatte, sondern vielmehr rechtswidriges Verhalten seiner Nutzer nach Möglichkeit zu verhindern suchte und damit den Schutz der Haftungsbeschränkung verdiente:

> „Perhaps most importantly, there is no indication that Veoh has failed to police its system to the fullest extent permitted by its architecture. ... [T]he record presented shows that Veoh has taken down blatantly infringing content, promptly responds to infringement notices, terminates infringing content on its system and its users' hard drives (and prevents that same content from being uploaded again), and terminates the accounts of repeat offenders. ... Once the content has been identified as infringing, Veoh's digital fingerprinting technology also prevents the same infringing content from ever being uploaded again. All of this indicates that Veoh has taken steps to reduce, not foster, the incidence of copyright infringement on its website."[1026]

(2) Unmittelbarer wirtschaftlicher Vorteil

Fraglich ist weiterhin, ob im Falle von Web 2.0-Diensten die zusätzliche Voraussetzung gemäß § 512(c)(1)(B) erfüllt ist, dass der ISP von dem rechtswidrigen Verhalten der Nutzer wirtschaftlich profitieren muss.

Insoweit könnte argumentiert werden, dass Web 2.0-Dienste aufgrund der Tatsache, dass sie oftmals auf einem werbefinanzierten Geschäftsmodells basieren, grundsätzlich von jedem unerlaubt hochgeladenen urheberrechtlich geschützten

1025 *IO Group, Inc. v. Veoh Networks, Inc.*, 2008 U.S. LEXIS 65915 (N.D. Cal. 2008).
1026 2008 U.S. LEXIS 65915, *55, 56.

Material profitieren, soweit dieses die Attraktivität ihrer Dienste für bestehende und neue Nutzer erhöht. Insoweit ist jedoch zu berücksichtigen, dass nach der Vorgabe des Gesetzgebers eine Gesamtbetrachtung des Internetdienstes des ISPs dahingehend anzustellen ist, ob dieser im Grunde genommen ein „seriöses" Geschäft betreibt. Auch darf der ISP nicht dafür bestraft werden, dass er sich für ein bestimmtes Geschäftsmodell entschieden hat. Wenn somit keine weiteren Umstände vorliegen, die belegen, dass der ISP einen wirtschaftlichen Vorteil aus den innerhalb seines Internetdienstes stattfindenden Rechtsverletzungen ziehen will, ist das Ausschlusskriterium gemäß § 512(c)(1)(B) nicht erfüllt.

Wenn ein ISP im Rahmen seines Internetdienstes Content-Identification-Technologien einsetzt und damit aktive Maßnahmen zur Verhinderung oder zumindest Eindämmung von Urheberrechtsverletzungen ergreift, geht daraus eindeutig hervor, dass er den Erfolg seines Dienstes nicht von den Rechtsverletzungen der Nutzer abhängig machen will. Aus diesem Grund ist das Vorliegen der Voraussetzung des unmittelbaren wirtschaftlichen Vorteils in Bezug auf einen Web 2.0-Dienst, der Content-Identification-Technologien innerhalb seines Dienstes einsetzt, bei Auslegung von § 512(c)(1)(B) entsprechend der gesetzgeberischen Vorgaben zu verneinen. Hingegen spricht der bewusste Verzicht auf Content-Identification-Technologien dafür, dass der ISP zumindest in gewissem Umfang dazu bereit ist, aus dem rechtswidrigen Material, das in seinem Internetdienst vorhanden ist, einen wirtschaftlichen Vorteil zu ziehen.

(3) Ergebnis

Das Ergebnis der Prüfung der Anwendbarkeit des Ausschlusskritieriums gemäß § 512(c)(1)(B) auf Web 2.0-Dienste unter Berücksichtigung der Verfügbarkeit von Content-Identification-Technologien läßt sich somit wie folgt zusammenfassen: Ein Web 2.0-Dienst, der Content-Identification-Technologien nicht einsetzt, verfügt bereits nicht über das erforderliche Maß an faktischer Kontrolle über das rechtswidrige Verhalten der Nutzer, weswegen das Ausschlusskriterium bereits aus diesem Grund nicht eingreift. Hingegen ist im Falle eines ISPs, der Content-Identification-Technologien einsetzt, von einer die Anforderungen von § 512(c)(1)(B) erfüllenden Kontrollmöglichkeit auszugehen. Allerdings ist in seinem Fall das Vorliegen der weiteren Voraussetzung des unmittelbaren wirtschaftlichen Vorteils zu verneinen, da er einen „seriösen" Dienst betreibt, bei dem auf den Schutz von Urheberrechten Wert gelegt wird und auch entsprechende Maßnahmen ergriffen werden, um den Eintritt von Rechtsverletzungen nach Möglichkeit zu verhindern.

f. Einhaltung des Verfahrens gemäß § 512(c)(1)(C)

Weiterhin muss der ISP, sobald er von einem Rechtsinhaber bzw. dessen Bevollmächtigten nach den Vorgaben des Verfahrens gemäß § 512(c)(1)(C) i.V.m. §§ 512(c)(3), 512(g) (nachfolgend "Notice&Takedown-Verfahren") über eine Rechtsverletzung in Kenntnis gesetzt wurde, unverzüglich das rechtsverletzende Material aus seinem System oder Netzwerk entfernen oder den Zugang hierzu sperren und den betroffenen Nutzer über die Beseitigung des von ihm hochgeladenen Materials informieren.

aa. Zweck

Nach dem Notice&Takedown-Verfahren haftet ein ISP, der auf eine Benachrichtigung des Rechtsinhabers hin urheberrechtswidriges Material unverzüglich aus seinem Internetdienst entfernt und den betroffenen Nutzer hierüber in Kenntnis setzt, weder gegenüber dem Rechtsinhaber für die Urheberrechtswidrigkeit des Materials noch gegenüber dem Nutzer für dessen Entfernung. Der ISP bleibt somit in Bezug auf den Konflikt zwischen dem Rechtsinhaber und dem Nutzer bezüglich der Rechtswidrigkeit des Materials außen vor.[1027]

Mit der Einführung des Notice&Takedown-Verfahrens beabsichtigte der US-amerikanische Gesetzgeber einen effizienten, kooperativen Prozess zum Umgang mit Rechtsverletzungen im Internet zu schaffen.[1028] Einerseits sollten die Rechtsinhaber die Möglichkeit erhalten, Urheberrechtsverletzungen möglichst einfach und zügig beseitigen lassen zu können. Andererseits sollten die ISPs Rechtssicherheit darüber erhalten, dass sie, sofern sie bestimmte Regeln befolgen, grundsätzlich weder Ansprüchen der Rechtsinhaber noch der Nutzer wegen des Vorhandenseins oder der Beseitigung von rechtswidrigem Material ausgesetzt sind.[1029] Weiterhin sollten durch das Verfahren Anreize für eine Zusammenarbeit zwischen ISPs und Rechtsinhabern zum Zwecke der Aufdeckung und Beseitigung von Urheberrechtsverletzungen geschaffen werden.[1030]

1027 Vgl. ausführlich zu den Voraussetzungen des Notice&Takedown-Verfahrens *Holznagel*, GRUR Int 2007, 971ff.
1028 H.R. Rep. 105-551(II), S. 54.
1029 *Ott*, GRUR Int. 2008, 563, 565.
1030 H.R. Rep. 105-551(II), S. 49.

bb. Struktur

Gemäß § 512(c)(3)(A) ist für das Vorliegen einer formal korrekten Benachrichtigung („Takedown-Notice") erforderlich, dass darin das urheberrechtlich geschützte Werk sowie das angeblich die Rechte an diesem Werk verletzende Material, das sich in dem Internetdienst des ISP befindet, bezeichnet wird.[1031] Das angeblich rechtsverletzende Material muss der Rechtsinhaber so genau identifizieren, dass es der ISP auf Grundlage dieser Information ohne weiteres auffinden und beseitigen kann. Damit legt das Gesetz die Last der Lokalisierung von rechtswidrigem Material innerhalb von Internetdiensten grundsätzlich den Rechtsinhabern auf.[1032] Hingegen trifft einen ISP, der die Anforderungen der Safe-Harbor-Regelung erfüllt, grundsätzlich keine Verpflichtung, darüber hinaus weitere Maßnahmen zur Aufdeckung oder Verhinderung von Urheberrechtsverletzungen zu treffen.[1033]

Entsprechend dieser Zielsetzung kann sich eine Takedown-Notice auch immer nur auf eine konkrete, bereits erfolgte angebliche Rechtsverletzung beziehen, hingegen keine Wirkung in Bezug auf zukünftige Rechtsverletzungen zeitigen, selbst wenn diese das gleiche urheberrechtlich geschützte Werk betreffen. Denn anderenfalls würde dem ISP faktisch eine Überwachungspflicht ab dem Zeitpunkt obliegen, in dem ihm eine Rechtsverletzung bezüglich eines urheberrechtlich geschützten Werks einmal angezeigt wurde. Eine solche Ausdehnung der zeitlichen und sachlichen Wirkung der Takedown-Notice widerspräche jedoch der grundsätzlichen Pflichtenverteilung, wonach die Last des Auffindens und der Anzeige konkreter Rechtsverletzungen den Rechtsinhabern obliegt.[1034] Darüber hinaus würde dies auch dem Ausschluss allgemeiner Überwachungspflichten des gemäß § 512(m)(1) widersprechen.[1035]

cc. Rechtsfolgen

Die Durchführung des Notice&Takdown-Verfahrens ist freiwillig, d.h. es besteht keine Pflicht weder seitens des ISPs noch des Rechtsinhabers, dessen Vorgaben

1031 Vgl. 17 U.S.C. § 512(c)(3)(A) (ii) und (iii).
1032 *VerSteeg*, 9 N.C. J.L. & Tech. 43, 58; *Reese*, 34 Sw. U. L. Rev. 287, 294 (2004); *Darrow/Ferrera*, 6 Nw. J. Tech. & Intell. Prop. 1, 16/17; *Katyal*, 32 Colum. J.L. & Arts, 401, 405 (2009); *Holznagel*, GRUR Int 2007, 971, 977: *Universal Recordings, Inc. v. Veoh Networks Inc.,* 2009 U.S. Dist. LEXIS 86932, *35 (C.D. Cal. 2009).
1033 *Ginsburg*, 50 Ariz. L. Rev. 577, 590-91 (2008).
1034 *Hendrickson v. Amazon*, 289 F.Supp.2 d 914, 916-917 (C. D. Cal. 20003): *„[I]t was not the intention of Congress that a coypright owner could write one blanket notice to all service providers alerting them of infringing material, thus, relieving him of any further responsibility and, thereby, placing the onus forever on the ISP."*
1035 Vgl. 8. Kapitel, Teil B.III.3.b.

einzuhalten. Allerdings spielt das Notice&Takedown-Verfahren für den Rechtsinhaber eine wichtige Rolle dabei, die Kenntnis des ISPs von rechtswidrigem Material im Sinne von § 512(c)(1)(A) nachzuweisen und damit dem ISP den Anspruch auf die Haftungsbeschränkung abzuschneiden.[1036] Kann der Rechtsinhaber diesen Nachweis nicht führen, ist der ISP im Falle des Vorliegens auch aller weiteren Voraussetzungen der Safe-Harbor-Regelung weitgehend vor den Folgen einer Haftung für Urheberrechtsverletzungen der Nutzer gefeit.[1037] Andererseits bringt sich ein Host-Provider, der sich entschließt, nach Erhalt einer Takedown-Notice das darin bezeichnete Material in seinem Internetdienst zu belassen, im Falle des tatsächlichen Vorliegens einer Rechtsverletzung um den weitgehenden Schutz, den die Safe-Harbor-Regelung ihm in Bezug auf die Haftung für Urheberrechtsverletzungen gewährt.[1038] Denn aufgrund der Unanwendbarkeit der Haftungsbeschränkung kann er sich dann zur Verteidigung gegen den Vorwurf des *copyright infringement* nur noch auf die allgemeingültigen Haftungsregeln berufen.[1039]

5. Ergebnis

Die Analyse der einzelnen Tatbestandsvoraussetzungen der Haftungsbeschränkung gemäß § 512(c) hat gezeigt, dass Web 2.0-Dienste grundsätzlich vom sachlichen und persönlichen Anwendungsbereich dieser Safe-Harbor-Regelung erfasst werden.

In Bezug auf die Auswirkungen von Content-Identification-Technologien auf die Anwendbarkeit der weiteren Voraussetzungen der Haftungsbeschränkung wurde zum einen gezeigt, dass Content-Identification-Technologien derzeit noch nicht als STMs im Sinne von § 512(i)(1)(B) qualifiziert werden können. Dies bedeutet, dass ihr Einsatz keine grundsätzliche Voraussetzung dafür ist, dass sich der Betreiber eines Web 2.0-Dienstes auf § 512(c) berufen kann.

Zum anderen hat die Prüfung der subjektiven Voraussetzungen gemäß § 512(c)(1)(A) ergeben, dass die Verfügbarkeit von Content-Identification-Technologien grundsätzlich keine Auswirkungen auf deren Beurteilung hat. Weder der Einsatz von Content-Identification-Technologien noch der bewusste Verzicht hierauf indiziert das (Nicht-)Vorliegen von positiver Kenntnis oder Umstandskenntnis des Web 2.0-Dienstes von in seinem Internetdienst begangenen Urheberrechtsverletzungen. Insbesondere darf von der Tatsache des Nichteinsatzes von Content-Identification-Technologien nicht auf ein vorsätzliches Sichverschließen des Web 2.0-

1036 Vgl. 8. Kapitel, Teil B.III.4.d.aa.(1).
1037 *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.04[A][3], S. 12B-58.
1038 *Nimmer*, in: Nimmer on Copyright, 2009, § 12B.04[A][3], S. 12B-58.
1039 *Holznagel*, GRUR Int 2007, 971, 978.

Dienstes vor Kenntnis von einer Rechtsverletzung im Sinne von § 512(c)(1)(A)(ii) geschlossen werden, vor allem deswegen, weil damit der ISP entgegen dem Ausschluss proaktiver Überwachungspflichten gemäß § 512(m) zum Einsatz solcher Technologien und damit zur Überwachung seines Dienstes auf Urheberrechtsverletzungen verpflichtet würde.

Die Prüfung des Ausschlusskriteriums gemäß § 512(c)(1)(B) hat gezeigt, dass der Einsatz von Content-Identification-Technologien die Gefahr birgt, dass aufgrund dieses Umstandes die Anwendbarkeit der Haftungsbeschränkung ausgeschlossen wird. Die Anwendbarkeit der Safe-Harbor-Regelung auf den Web 2.0-Dienst hängt vor allem davon ab, welche Anforderungen an das Kriterium des unmittelbaren wirtschaftlichen Vorteils gestellt werden, vor dem Hintergrund, dass Web 2.0-Dienste, die oftmals auf einem werbefinanzierten Geschäftsmodell basieren, grundsätzlich von jedem unerlaubt hochgeladenen urheberrechtlich geschützten Material profitieren, wenn dieses Material die Attraktivität ihres Dienstes für die Nutzer erhöht. Lässt man diesen Umstand in Anlehnung an das für die begrifflich identische Voraussetzung der *vicarious liability* entwickelte *case law* zur Erfüllung des Kriteriums ausreichen, sind Web 2.0-Dienste, die sich besonders um den Schutz von Urheberrechten durch den Einsatz von Content-Identification-Technologien bemühen, regelmäßig von dem Schutz der Haftungsbeschränkung gemäß § 512(c) ausgeschlossen.

IV. Zusammenfassung der Ergebnisse betreffend die Haftung von Web 2.0-Diensten nach US-amerikanischem Urheberrecht

In Bezug auf die Haftung von Web 2.0-Diensten für die Rechtsverletzungen ihrer Nutzer nach US-amerikanischem Urheberrecht ergibt sich ein differenziertes Bild, je nachdem, ob der den Internetdienst betreibende ISP eine Content-Identification-Technologie einsetzt oder nicht.

1. Haftung eines Web 2.0-Dienstes, der keine Content-Identification-Technologien einsetzt

Auf der Ebene der Haftungsbegründung besteht für einen Web 2.0-Dienst, der innerhalb seines Internetdienstes keine Content-Identification-Technologie einsetzt, ein erhebliches Risiko, dass er aufgrund dieses Umstandes als *contributory infringer* auf der Grundlage der *inducement rule* für die innerhalb seines Internetdienstes begangenen Urheberrechtsverletzungen der Nutzer haftbar gemacht wird.

Hingegen wirkt sich der Umstand des Nichteinsatzes von Content-Identification-Technologien im Rahmen der Haftungsbeschränkung gemäß § 512(c) nicht zu seinem Nachteil aus. Denn sowohl im Rahmen der subjektiven Voraussetzungen gemäß § 512(c)(1)(A) als auch in Bezug auf die Voraussetzung der tatsächlichen Beherrschungsmöglichkeit gemäß § 512(c)(1)(B) darf die theoretische Möglichkeit des Einsatzes von Content-Identification-Technologien wegen des Ausschlusses proaktiver Überwachungspflichten gemäß § 512(m) nicht zu Lasten des ISPs berücksichtigt werden. Das Gebot, dass ISPs durch die Safe-Harbor-Regelung in keiner Weise zur Überwachung bzw. zur Durchsuchung ihrer Internetdienste auf Umstände, die auf Rechtsverletzungen der Nutzer hinweisen, verpflichtet werden sollen, gilt ohne Einschränkung. Denn Content-Identification-Technologien erfüllen bisher noch nicht die Anforderungen, die das Gesetz an das Vorliegen einer STM im Sinne von § 512(i)(1)(B) stellt.

Dies bedeutet, dass ein Web 2.0-Dienst, der in seinem Internetdienst keine Content-Identification-Technologie einsetzt, zwar auf der Ebene der Haftungsbegründung für eine Haftung anfällig ist, die Folgen dieser Haftung aufgrund des Eingreifens von § 512(c) aber weitgehend beschränkt werden.

2. Haftung eines Web 2.0-Dienstes, der eine Content-Identification-Technologie einsetzt

Hingegen erfüllt ein Web 2.0-Dienst, der eine Content-Identification-Technologie innerhalb seines Internetdiensts einsetzt, auf der Ebene der Haftungsbegründung die Voraussetzungen der *vicarious liability*. Denn wegen des Einsatzes der Technologie, die die Identifikation und Blockierung von urheberrechtswidrigem Material bereits im Rahmen des Hochladevorgangs erlaubt, verfügt der ISP über die tatsächliche Möglichkeit, das rechtswidrige Verhalten der Nutzer zu kontrollieren. Aufgrund ihres werbebasierten Geschäftsmodells erfüllen Web 2.0-Dienste regelmäßig die Voraussetzung des unmittelbaren wirtschaftlichen Vorteils, die im Rahmen der *vicarious liability* sehr weit ausgelegt wird.

Auf der Ebene der Haftungsbeschränkung droht die Anwendbarkeit von § 512(c) sodann entsprechend am Ausschlusskriterium gemäß § 512(c)(1)(B) zu scheitern, dessen Voraussetzungen mit denjenigen der *vicarious liability* begrifflich identisch sind. Insoweit hat die Analyse jedoch ergeben, dass nach der gesetzgeberischen Intention im Rahmen der Haftungsbeschränkung insbesondere unter der Voraussetzung des unmittelbaren wirtschaftlichen Vorteils im Sinne von § 512(c)(1)(B) etwas anderes zu verstehen ist als im Rahmen der gleichlautenden Haftungsvoraussetzungen der *vicarious liability*. Denn ISPs, die um den Schutz von Urheberrechten bemüht sind und damit ein „seriöses Geschäft“ betreiben, sol-

len gerade nicht vom Anwendungsbereich von § 512(c) ausgeschlossen werden. Erforderlich ist somit eine ganzheitliche Betrachtung des Geschäftsgebahrens des ISPs, die ergeben muss, dass der Internetdienst gezielt darauf angelegt ist, von den Urheberrechtsverletzungen der Nutzer zu profitieren. Hierfür bestehen jedoch im Falle eines ISPs, der freiwillig eine Content-Identification-Technologie einsetzt, um Urheberrechtsverletzungen innerhalb seines Internetdienstes von vornherein auszuschließen, regelmäßig keine Anhaltspunkte. Daher müssten die Gerichte bei richtiger Auslegung der Voraussetzungen von § 512(c) zu dem Ergebnis kommen, dass auch ein ISP, der Content-Identification-Technologien einsetzt, die Haftungsbeschränkung für sich beanspruchen kann. Insoweit kann die Entscheidung des Gerichts in *IO v. Veoh* als Vorbild dienen, worin das Gericht zu folgendem Ergebnis kam:

> „...the issue is whether Veoh takes appropriate steps to deal with copyright infringement that takes place. The record presented demonstrates that, far from encouraging infringement, Veoh has a strong DMCA policy, takes steps to limit incidents of infringement on its website and works diligently to keep unauthorized works off its website. In sum, Veoh has met its burden in establishing its entitlement to safe harbor for the alleged infringements here."[1040]

Aufgrund der begrifflichen Identität der Voraussetzungen des Ausschlusskriteriums gemäß § 512(c)(1)(B) und denjenigen der *vicarious liability* besteht auf Seiten von ISPs, die Content-Identification-Technologien einsetzen, jedoch ein erhebliches Risiko, dass sich ein Gericht bei dessen Auslegung allein an dem zur *vicarious liability* ergangenen *case law* orientieren wird und auf dieser Grundlage zu dem Ergebnis kommt, dass die Voraussetzungen des Ausschlusskriteriums erfüllt sind und damit die Haftungsbeschränkung auf den Web 2.0-Dienst unanwendbar ist.

Dies bedeutet für einen Web 2.0-Dienst, der im Rahmen des Dienstes Content-Identification-Technologien einsetzt, dass diese Tatsache nicht nur dazu führt, dass er dem Grunde nach als *vicarious infringer* für die Rechtsverletzungen der Nutzer haftet, sondern darüber hinaus extrem gefährdet ist, den Schutz der Haftungsbeschränkung gemäß § 512(c) zu verlieren.

3. Ergebnis

Aus der vorhergehenden Analyse folgt, dass im Ergebnis ISPs, die sich bewusst gegen den Einsatz von Content-Identification-Technologien entscheiden, durch die Safe-Harbor-Regelung besser geschützt werden als ISPs, die sich dafür entschei-

1040 *IO Group, Inc. v. Veoh Networks, Inc.*, 2008 U.S. Dist. LEXIS 65915, **61 (N.D. Cal. 2008).

den, durch den Einsatz solcher Technologien ein höheres Schutzniveau für Urheberrechte zu schaffen. Denn das Wohl und Wehe des ISPs, der Content-Identification-Technologien einsetzt, hängt in Bezug auf die Frage, ob die Safe-Harbor-Regelung auf ihn anwendbar ist, von der Gunst und der Gründlichkeit des befassten Gerichts bei der Auslegung des Ausschlusskriteriums gemäß § 512(c)(1)(B) ab. Hingegen bietet die Safe-Harbor-Regelung keinerlei Angriffsflächen, um ISPs, die keine Content-Identification-Technologien einsetzten, aufgrund dieses Umstands vom Schutz der Haftungsbeschränkung zu disqualifizieren. Dieses Ergebnis ist nicht interessengerecht.[1041]

a. Kritik am threshold requirement gemäß § 512(i)(1)(B)

Diese Schieflage ist zum einen das Ergebnis der verunglückten Regelung betreffend das *threshold requirement* der STMs. Denn dieses als Korrektiv gedachte Konstrukt, über das zukünftige technologische Entwicklungen berücksichtigt werden und gegebenenfalls auch Überwachungspflichten zu Lasten von ISPs entstehen sollten, wurde in seiner Entstehung von der Kooperation der ISPs und damit gerade derjenigen abhängig gemacht, deren rechtliche und wirtschaftliche Position durch die Entstehung solcher STMs negativ beeinflusst wird. Damit hat der Gesetzgeber die Voraussetzungen dafür geschaffen, dass diejenigen, deren Position durch STMs verschlechtert würde, die Entstehung von STMs und damit einer Verpflichtung der ISPs zur Überwachung ihrer Internetdienste auf Urheberrechtsverletzungen verhindern können. Dies sind vor allem die ISPs, die nach der durch den DMCA derzeit vorgesehenen Verteilung der Lasten des *copyright policing* im Wesentlichen lediglich das Notice&Takedown-Verfahren einhalten müssen, um von einer Haftung für Rechtsverletzungen, die die Nutzer innerhalb und mit Hilfe ihrer Internetdienste begehen, weitgehend verschont zu bleiben. Hingegen ist es allein den Rechtsinhabern überlassen, sämtliche Internetdienste nach Verletzungen ihrer urheberrechtlich geschützten Werke zu durchsuchen und diese den ISPs zur Kenntnis zu bringen.

Ziel der Schaffung der STMs war jedoch, einen besseren Schutz von Urheberrechten durch die Beförderung der Entwicklung entsprechender Technologien zu gewährleisten. Um dieses Ziel auch tatsächlich zu erreichen, hätte im Gesetz zunächst klargestellt werden müssen, dass die Safe-Harbor-Regelung nur solange und soweit Geltung beanspruchen kann, wie es ISPs tatsächlich nicht möglich ist, den innerhalb ihrer Internetdienste stattfindenden Datenverkehr zu kontrollieren und dadurch Urheberrechtsverletzungen zu verhindern. Weiterhin müsste das Gesetz

1041 So auch *Beaty*, 13 Marq. Intell. Prop. L. Rev. 207, 226 (2009); *Ott*, GRUR Int. 2008, 563, 567.

ein Verfahren vorsehen, über das sichergestellt wird, dass die betroffenen Interessengruppen sich unabhängig von den daraus resultierenden Auswirkungen auf ihre Rechtspositionen an der Entwicklung von zweckdienlichen STMs beteiligen oder zumindest dazu gezwungen werden können, bereits fertig entwickelte, effektive Technologien als STMs im Rahmen ihrer Internetdienste einzusetzen. Innerhalb dieses Verfahrens müsste auch geprüft werden, ob eine als STM vorgeschlagene Technologie faktisch in der Lage ist, Urheberrechte zu schützen und damit eine Verpflichtung der ISPs zum Einsatz der Technologie zu rechtfertigen. Denn grundsätzlich sollte für die Qualifizierung als STM weniger eine Rolle spielen, in welchem Verfahren eine Technologie entwickelt wurde, als die Frage, ob die Technologie den Schutz von Urheberrechten in der Tat effektiv verbessern kann.

b. Kritik an der Ausgestaltung des Ausschlusskriteriums gemäß § 512(c)(1)(B)

Zum anderen muss das Ausschlusskriterium gemäß § 512(c)(1)(B) ausdifferenziert und von den begrifflich identischen Voraussetzungen der *vicarious liability* inhaltlich deutlich abgegrenzt werden.

Denn aufgrund der Identität der Voraussetzungen besteht die Gefahr, dass von den Gerichten der unterschiedliche Kontext, in dem diese Begriffe verwendet werden, nicht ausreichend berücksichtigt wird. Damit wird jedoch vor allem die Findung interessengerechter Lösungen im Rahmen der Safe-Harbor-Regelung gefährdet. Denn das *case law* zur *vicarious liablity* bietet keine angemessene Grundlage zur Beurteilung der Legitimität eines Web 2.0-Dienstes. Dies liegt vor allem an der im Rahmen der *vicarious liability* ausufernd weiten Auslegung der Voraussetzung des unmittelbaren wirtschaftlichen Vorteils. Denn gerade im Web 2.0 verschwimmen zunehmend die Grenzen zwischen mittelbaren und unmittelbaren wirtschaftlichen Vorteilen aufgrund der zunehmenden Verbreitung von werbebasierten Geschäftsmodellen. Es müsste daher klargestellt werden, dass von dem Schutz der Haftungsbeschränkung gemäß § 512(c) nur solche ISPs auszuschließen sind, deren Geschäftsmodell gezielt auf die Begehung von Urheberrechtsverletzungen durch die Nutzer angelegt ist.

c. Zusammenfassung

Durch die beiden vorgeschlagenen Modifikationen der Anwendungsvoraussetzungen für die Haftungsbeschränkung gemäß § 512(c) würde ein gerechter Ausgleich zwischen den widerstreitenden Interessen von Rechtsinhabern und ISPs in Bezug auf den Schutz von Urheberrechten wiederhergestellt. ISPs, die auf den durch das

Internet und die Digitalisierung geschaffenen technischen Möglichkeiten ein Geschäft aufbauen und damit ihr Geld verdienen, könnten durch eine Modifizierung der Definition von STMs dazu verpflichtet werden, im Gegenzug die damit verbundenen Nachteile für die Rechtsinhaber einzudämmen. Darüber hinaus erhielten ISPs, die sich freiwillig um einen besseren Schutz von Urheberrechten bemühen, durch eine Konkretisierung des Ausschlusskriteriums gemäß § 512(c)(1)(B) die Sicherheit, dass sie durch ihre im Sinne des Urheberrechtsschutzes begrüßenswerten, freiwilligen Maßnahmen keine Nachteile erleiden werden. Denn zu ihren Gunsten würde berücksichtigt, dass sie keinen Internetdienst betreiben, der auf der Begehung von Urheberrechtsverletzungen durch die Nutzer aufbaut, sondern vielmehr, dass sie sich um den Urheberschutz besonders bemühen.

4. Bewertung der Aussichten der Klage von Viacom gegen YouTube auf der Grundlage der gefundenen Ergebnisse

Mit der Klage gegen YouTube verfolgt Viacom offensichtlich das Ziel, einen der prominentesten Internetdienste des Web 2.0 im Wege einer gerichtlichen Entscheidung dazu verpflichten zu lassen, über die Einhaltung der Vorgaben des Notice&Takedown-Verfahrens hinaus proaktiv in Bezug auf die Auffindung und zukünftigen Verhinderung von Urheberrechtsverletzungen tätig zu werden. Damit wird der *status quo* in Bezug auf die Verteilung der Lasten des *copyright policing* zwischen Rechtsinhabern und ISPs auch in rechtlicher Hinsicht in Frage gestellt.[1042] Hätte Viacom mit dieser Strategie bei dem Gericht Erfolg, so würde dies weitreichende Konsequenzen für das zukünftige Verhältnis zwischen Rechtsinhabern und Host-Providern nach sich ziehen.[1043]

Allerdings hat die Analyse der Haftung von Web 2.0-Diensten für die Rechtsverletzungen der Nutzer nach derzeitigem US-amerikanischem Urheberrecht gezeigt, dass das Bestreben von Viacom kaum rechtlich begründet werden kann. Denn nach der derzeitigen Rechtslage, die vor allem durch die Haftungsbeschränkung gemäß § 512(c) geprägt ist, obliegt die Last des *copyright policing* klar den Rechtsinhabern. Dies zeigt sich insbesondere an der Ausgestaltung des Notice&Take-

1042 *Meisel*, Journal of Internet Law, Volume 12, Number 8, February 2009, p. 1, 13.

1043 Fred von Lohmann, Anwalt und Sprecher der Electronic Frontier Foundation, befürchtet in diesem Fall einen tiefgreifenden Rückschritt für Web 2.0-Dienste insoweit, dass die Anbieter dieser Dienste gezwungen wären, zur Minimierung ihres Haftungsrisikos jeden einzelnen Inhalt vor seiner Veröffentlichung auf ihrem Dienst zu prüfen: *„In other words, a decisive victory for Viacom could potentially turn the Internet into TV, a place where nothing gets on the air until a cadre of lawyers signs off*", so zitiert in Chaqui Cheng, Viacom, Google set for fight to bitter end over Safe Harbor, Ars Technica, 7.5.2008, http://arstechnica.com/news.ars/post/20080507-viacom-google-set-for-fight-to-bitter-end-over-safe-harbor.html (abgerufen am 01.07.2010).

down-Verfahrens gemäß § 512(c)(3), und darüber hinaus an dem Ausschluss allgemeiner Überwachungspflichten, der in § 512(m) zum Ausdruck kommt. In diesen beiden Regelungen kommt die Absicht des Gesetzgebers zum Ausdruck, die Last der Suche nach und der Lokalisierung von Rechtsverletzungen den Rechtsinhabern aufzuerlegen; ISPs sind insoweit lediglich verpflichtet, Rechtsverletzungen nach ihrer Lokalisierung und Anzeige durch die Rechtsinhaber möglichst schnell zu beseitigen. Ein Gericht müsste sich über diese klare Entscheidung, Rechtsinhabern die Last des *copyright policing* aufzuerlegen, bewusst hinwegsetzen, um Viacom zum Sieg zu verhelfen. Deswegen wird teilweise vermutet, dass Viacom es darauf anlegt, das Verfahren zunächst zu verlieren und die wesentlichen Rechtsfragen sodann durch den Instanzenzug bis vor den Supreme Court zu bringen, um dort die in § 512(c) niedergelegte Lastenverteilung in Bezug auf das *copyright policing* grundsätzlich in Frage stellen zu können.[1044]

Dementsprechend hat das erstinstanzlich mit dem Verfahren befasste Gericht in seinem Urteil vom 23. Juni 2010 die Klage abgewiesen.[1045] Die Klageabweisung wurde damit begründet, dass infolge des Eingreifens der Haftungsbeschränkung gemäß § 512(c) keinerlei Ansprüche wegen *primary* und *secondary infringement* gegen YouTube geltend gemacht werden könnten. Das Gericht verneinte insbesondere, dass seitens YouTube das erforderliche Maß an Kenntnis von Rechtsverletzungen vorliegt, durch das der Web 2.0-Dienst gemäß § 512(c)(1)(A) vom Schutz der Haftungsbeschränkung ausgeschlossen werden könnte. Denn hierfür müsse konkrete Kenntnis von bestimmten Rechtsverletzungen gegeben sein und nicht nur ein generelles Bewusstsein seitens YouTube, dass sein Internetdienst auch zu rechtswidrigen Zwecken genutzt wird.[1046] In diesem Zusammenhang schloss das Gericht mit Verweis auf den Ausschluss allgemeiner Überwachungspflichten gemäß § 512(m)(1) auch ausdrücklich eine Pflicht seitens YouTube aus, auf seiner Webseite befindliches Material auf seine Rechtswidrigkeit hin überprüfen zu müs-

1044 *Rosenblatt*, YouTube Emails Discovered in Viacom Case: Smoking Gun or Wet Blanket?, Copyright and Technology, 8.10.2009, http://copyrightandtechnology.com/2009/10/08/youtube-emails-discovered-in-viacom-case-smoking-gun-or-wet-blanket/ (abgerufen am 01.07.2010).

1045 Viacom Int'l Inc., et al., v. YouTube, Inc., et al., Nos. 07-Civ-2103 (LLS), 07-Civ-3582 (LLS) Opinion and Order (S.D.N.Y. June 23, 2010).

1046 Viacom Int'l Inc., et al., v. YouTube, Inc., et al., Nos. 07-Civ-2103 (LLS), 07-Civ-3582 (LLS) Opinion and Order, S. 15 (S.D.N.Y. June 24, 2010), abrufbar unter http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/de//press/pdf/msj_decision.pdf (zuletzt abgerufen am 01.07.2010). Auf Content-Identification-Technologien ging das Gericht nur am Rande ein, nämlich im Zusammenhang mit der Frage, ob YouTubes Internetdienst die Anforderungen gemäß § 512(i)(1)(A) in Bezug auf die angemessene Implementierung einer *repeat infringers policy* erfüllte, was das Gericht im Ergebnis bejahte. An dieser Stelle fand Erwähnung, dass YouTube im Zusammenhang mit der „Claim Your Content"-Funktion, die den Rechtsinhabern im Rahmen des Internetdienstes zur Auffindung rechtswidrigen Materials zur Verfügung gestellt wird, ein „fingerprinting tool" von Audible Magic einsetzt.

sen.[1047] Auch sprach für die Anwendbarkeit der Safe-Harbor-Regelung zugunsten von YouTube nach Auffassung des Gerichts, dass konkretes rechtswidriges Material umgehend beseitigt wurde, sobald der Internetdienst auf solches innerhalb seines Internetdienstes befindliches Material von einem Rechtsinhaber aufmerksam gemacht wurde.[1048]

C. *Vergleich mit der deutsch-europäischen Rechtslage in Bezug auf die Haftung von Web 2.0-Diensten für Urheberrechtsverletzungen der Nutzer*

Nachfolgend wird zunächst die Haftung von Web 2.0-Diensten für Urheberrechtsverletzungen der Nutzer nach deutsch-europäischem Recht sowie die Auswirkungen der Verfügbarkeit von Content-Identification-Technologien hierauf dargestellt. Die Ergebnisse dieser Prüfung werden daraufhin mit der US-amerikanischen Rechtslage verglichen.

I. Die Haftung von ISPs für Urheberrechtsverletzungen nach deutsch-europäischem Recht

Werden im Internetdienst eines ISPs urheberrechtlich geschützte Multimediawerke durch einen Nutzer ohne Erlaubnis des Rechtsinhabers gespeichert und steht somit eine Verletzung von Urheberrechten im Raum, so richtet sich die Haftung des ISPs zuvorderst nach den speziellen urheberrechtlichen Haftungsregelungen gemäß §§ 97 ff. UrhG. Daneben kommt grundsätzlich auch eine Haftung nach den Regeln des allgemeinen Deliktsrechts gemäß §§ 823 ff. BGB sowie der allgemeinen Störerhaftung gemäß § 823 Abs. 1 i.V.m. § 1004 BGB in Betracht, da Urheberrechte in ihrer Eigenschaft als Immaterialgüterrechte sonstige Rechte im Sinne von § 823 Abs. 1 BGB darstellen.[1049] Gegenüber §§ 97 UrhG sind die Regelungen des allge-

1047 Viacom Int'l Inc., et al., v. YouTube, Inc., et al., Nos. 07-Civ-2103 (LLS), 07-Civ-3582 (LLS) Opinion and Order, S. 16 (S.D.N.Y. June 24, 2010).
1048 Viacom Int'l Inc., et al., v. YouTube, Inc., et al., Nos. 07-Civ-2103 (LLS), 07-Civ-3582 (LLS) Opinion and Order, S. 23 (S.D.N.Y. June 24, 2010).
1049 BGH vom 11.03.2004, GRUR 2004, 860, 864; *Sprau*, in: *Palandt*, BGB, 2010, § 823 Rn. 15.

meinen Deliktsrechts jedoch subsidiär und kommen nur bei Auftreten einer planwidrigen Regelungslücke zur Anwendung.[1050]

1. Schadensersatzhaftung gemäß § 97 Abs. 2 S. 1 UrhG

Im Falle der Verletzung von Urheberrechten innerhalb eines Web 2.0-Dienstes kommt zunächst ein Anspruch des Urhebers gegen den ISP auf Schadensersatz gemäß § 97 Abs. 2 S. 1 UrhG in Betracht. Ein Schadensersatzanspruch gemäß § 97 Abs. 2 S. 1 UrhG ist gegeben, wenn eine rechtswidrige, vorsätzliche Verletzung einer urheberrechtlich geschützten Rechtsposition vorliegt. Sind diese Tatbestandsvoraussetzungen erfüllt, kann der Urheber nach dem Grundsatz der dreifachen Schadensberechnung nach seiner Wahl vom Verletzer entweder Ersatz des konkreten Schadens gemäß § 97 Abs. 2 S. 1 UrhG i.V.m. §§ 249 ff. BGB oder Herausgabe des Verletzergewinns gemäß § 97 Abs. 2 S. 2 UrhG verlangen. Weiterhin kann er gemäß § 97 Abs. 2 S. 3 UrhG im Wege der sogenannten „Lizenzanalogie" Herausgabe desjenigen Betrages verlangen, den der Urheber als angemessene Vergütung hätte verlangen können, wenn der Verletzer vor der Vornahme der Verletzungshandlung eine entsprechende Erlaubnis eingeholt hätte. Zudem kommt in schwerwiegenden Fällen der Verletzung von Urheberpersönlichkeitsrechten ein Anspruch auf Ersatz des immateriellen Schadens aus Billigkeitsgründen gemäß § 97 Abs. 2 S. 4 UrhG in Betracht.

a. Multimediawerke als schutzfähige Werke im Sinne des UrhG

Zunächst müssen die im Rahmen von Web 2.0-Diensten von Nutzern eingestellten Multimediawerke, die, wie eingangs erläutert wurde,[1051] aus Musik- oder Filmwerken bzw. Kombinationen hieraus bestehen, urheberrechtlich schutzfähige persönliche geistige Schöpfungen im Sinne des UrhG darstellen.[1052]

Werke der Musik genießen gemäß § 2 Abs. 1 Nr. 2 UrhG urheberrechtlichen Schutz. Musikwerke in diesem Sinne sind Töne jeglicher Art, die von Menschen geschaffen wurden, d.h. eine „menschlich veranlasste Folge von Tönen".[1053]

1050 *Sprau*, in: *Palandt*, BGB, 2010, Einf v § 823 Rn. 9; *Mertens*, in: *Rebmann/Säcker* (Hrsg.) MüKo, BGB, 2004, § 823, Rn. 156, der jedoch den Rückgriff auf § 823 BGB im Falle einr Regelungslücke ablehnt; *Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 97 Rn. 225; *Buschle*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, Teil D, Rn. 257.

1051 Vgl. 1. Kapitel.

1052 Vgl. 5. Kapitel, Teil B.III.1.b.

1053 BGH vom 03.02.1988 GRUR 1988, 810, 811 – *Fantasy*; BGH vom 03.02.1988, GRUR 1988, 812, 814 – *Ein bisschen Frieden*; *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, § 2, Rn. 134; *A. Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 2, Rn. 122.

Schützbar ist die menschliche Stimme sowie der Einsatz von Instrumenten jeglicher Art, mit denen Töne, Geräusche oder Klänge erzeugt werden können.[1054] Auch elektronisch erzeugte Klänge können in ein Musikwerk einbezogen werden. Erforderlich ist, dass die musikalische Schöpfung eine wahrnehmbare Form gefunden hat, d.h. dass sie der Wahrnehmung durch die menschlichen Sinne zugänglich ist.[1055] Unerheblich ist insoweit die Art der Festlegung des Musikwerks, beispielsweise die Fixierung von Tönen in Notenschrift oder auf einem Tonträger.[1056] Auch eine unkörperliche Wahrnehmbarmachung, beispielsweise im Falle eines improvisierten Musikstücks, kann hierfür ausreichend sein.[1057] Neben demjenigen, der das Musikwerk geschaffen hat, können weitere Personen Rechte im Zusammenhang mit dem Musikwerk erwerben, wenn dieses auf einen Tonträger aufgenommen wird. So hat der ausübende Künstler, der das Musikwerk darbietet, gemäß § 77 Abs. 1 UrhG das ausschließliche Recht, diese Darbietung auf einen Tonträger aufzunehmen. Gemäß § 77 Abs. 2 UrhG steht ihm auch allein das Recht zu, den Tonträger, der seine Darbietung enthält, zu vervielfältigen und zu verbreiten. Darüber hinaus erwachsen dem Hersteller des Tonträgers gem. § 85 Abs. 1 UrhG spezielle Rechte, indem dieser ausschließlich dazu berechtigt ist, den Tonträger zu vervielfältigen, zu verbreiten und öffentlich zugänglich zu machen.

Weiterhin genießen gemäß § 2 Abs. 1 Nr. 5 UrhG auch Filmwerke urheberrechtlichen Schutz. Filmwerke in diesem Sinne sind Werke eigener Art, bei denen die benutzten Werke wie beispielsweise Sprach- und Musikwerke zu einer Einheit verschmolzen und ins Bildliche umgewandelt werden.[1058] Entscheidend ist das Vorliegen einer bewegten Bild- oder Bildtonfolge, die den Eindruck eines bewegten Bildes hervorruft.[1059] Unerheblich ist die Art der Aufnahmetechnik (digital oder analog) sowie der Inhalt des jeweiligen Films, so dass Kino- und Fernsehfilme, Dokumentarfilme, wissenschaftliche Filme, Werbefilme etc. von dieser Werkskategorie erfasst werden.[1060] Urheber des Filmwerks sind diejenigen natürlichen Personen, die an dessen Herstellung schöpferisch mitwirken, wie beispielsweise Regisseur, Kameramann, Cutter, Szenenbildner, Filmarchitekt, Kostümbildner und

1054 *Loewenheim*, in: *Schricker* (Hrsg.), UrhR, 2006, § 2, Rn. 118.
1055 *Czychowski*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 9, Rn. 67.
1056 *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, § 2, Rn. 135.
1057 *Czychowski*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 9, Rn. 67; *A. Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 2, Rn. 133; *Loewenheim*, in: *Schricker* (Hrsg.), UrhR, 2006, § 2, Rn. 118.
1058 *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, § 2, Rn. 204.
1059 *Nordemann*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 9, Rn. 161; *A. Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 2, Rn. 203; *Loewenheim*, in: *Schricker* (Hrsg.), UrhR, 2006, § 2, Rn. 181.
1060 *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, § 2, Rn. 205, 206; *Nordemann*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 9, Rn. 162; *Loewenheim*, in: *Schricker* (Hrsg.), UrhR, 2006, § 2, Rn. 181.

Filmtonmeister.[1061] Darüber hinaus erwerben die in einem Filmwerk mitwirkenden Schauspieler in ihrer Eigenschaft als ausübende Künstler Rechte an dem Filmwerk gemäß §§ 77 UrhG.

Es ergibt sich somit aus der vorstehenden Darstellung, dass Musik- und Filmwerke, die von Nutzern in Web 2.0-Dienste eingestellt werden, urheberrechtlichen Schutz genießen.

b. Verletzungshandlung

Voraussetzung für den urheberrechtlichen Schadensersatzanspruch ist zunächst die Verletzung eines fremden Urheberrechts.[1062] Eine solche Verletzungshandlung liegt insbesondere dann vor, wenn ein Nichtberechtigter in Bezug auf das urheberrechtlich geschützte Werk eine gemäß §§ 16 ff. UrhG ausschließlich dem Rechtsinhaber vorbehaltene Nutzungshandlung ohne dessen Erlaubnis vornimmt. Bei Handlungen, die im Kontext von Web 2.0-Diensten in Bezug auf Multimediawerke vorgenommen werden, kommt insbesondere eine Verletzung des Vervielfältigungsrechts gemäß § 16 Abs. 1 UrhG sowie des Rechts der öffentlichen Zugänglichmachung gem. § 19 a UrhG in Betracht.

aa. Vervielfältigungsrecht

§ 6 UrhG behält dem Rechtsinhaber das Recht vor, darüber zu entscheiden, ob und in welcher Form weitere Exemplare seines Werks hergestellt werden dürfen. Denn mit jeder Vervielfältigung vergrößert sich der Kreis derjenigen, die das Werk potentiell lesen, hören oder auf andere Weise wahrnehmen können.[1063] Unter dem Begriff der „Vervielfältigung" im Sinne von § 16 UrhG wird die Herstellung einer oder mehrerer körperlicher Festlegungen eines Werks verstanden, die geeignet sind, das Werk den menschlichen Sinnen auf irgendeine Weise wiederholt unmit-

1061 Sogenanntes „Mehrurheberwerk", vgl. *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, § 2, Rn. 218; *Nordemann*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 9, Rn. 179 f.; *A. Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 2, Rn. 201; *Loewenheim*, in: *Schricker* (Hrsg.), UrhR, 2006, § 2, Rn. 190.

1062 *Dreier*, in: *Schulze*/*Dreier*, UrhG, 2008, § 97 Rn. 3.

1063 Sogenannter „Multiplikationseffekt", vgl. *Dustmann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 16 UrhG Rn. 2.

telbar oder mittelbar wahrnehmbar zu machen.[1064] Maßgeblich ist die körperliche Fixierung des Werks in dem Vervielfältigungsstück.[1065] Auf die Art des Materials und des Herstellungsverfahrens – beispielsweise analog oder digital – kommt es hingegen nicht an.[1066] Das Vervielfältigungsrecht ist ein Verbotsrecht,[1067] d.h. wer ein fremdes Werk vervielfältigen will, muss sich hierfür das Recht vom Rechtsinhaber einräumen lassen, es sei denn, seine Vervielfältigungshandlung ist durch die gesetzlichen Schrankenbestimmungen gemäß §§ 44 a ff. UrhG legitimiert, was der Nutzer konkret darlegen und beweisen können muss.[1068]

Daraus folgt, dass von dem Vervielfältigungsrecht auch die Speicherung einer digitalen Kopie eines Werks auf einem Datenträger wie beispielsweise dem Server eines Internetdienstes erfasst wird.[1069] Lädt somit ein Nutzer eines Web 2.0-Dienstes, beispielsweise einer Videoplattform, eine Datei, die ein urheberrechtlich geschütztes digitales Filmwerks enthält, auf den Server des die Videoplattform betreibenden ISPs hoch, erstellt er im Zuge dieses Vorgangs ein Vervielfältigungsstück des Filmwerks und verstößt damit gegen § 16 UrhG.[1070] Ebenso fällt das Downloaden, wie beispielsweise das Herunterladen eines digitalen Multimediawerks von der Webseite einem Web 2.0-Dienstes auf den Computer des Nutzers, unter § 16 UrhG.[1071]

1064 BGH vom 18.05.1955, GRUR 1955, 492, 494 – *Grundig Reporter*; BGH vom 01.07.1982, GRUR 1983, 28, 29 – *Presseberichterstattung und Kunstwerkwiedergabe II*; BGH vom 04.10.1990, GRUR 1991, 449, 453 – *Betriebssystem*; BGH GRUR vom 04.05.2000, GRUR 2001, 51, 52 – *Parfumflakon*; *Dustmann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 16 UrhG Rn. 9; *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, § 16 Rn. 6; *Loewenheim*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 20, Rn. 4.

1065 *Loewenheim*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 20, Rn. 4; *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, § 16 Rn. 6.

1066 *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, § 16 Rn. 7; *Loewenheim*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 20, Rn. 5; .

1067 *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, § 16 Rn. 18.

1068 BGH vom 10.07.1986, GRUR 1986, 887, 888 – *BORA BORA*.

1069 BGH vom 10.12.1998, GRUR 1999, 325 – *Elektronische Pressearchive*; OLG München vom 08.03.2000, GRUR 2001, 499, 503 – *MIDI-Files*; KG vom 27.08.2002, MMR 2003, 110, 112 – *Paul und Paula*; *Dustmann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 16 UrhG Rn. 26; *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, § 16 Rn. 15.

1070 Zur Bereitstellung von Filmausschnitten im Internet vgl. KG vom 27.08.2002, MMR 2003, 110, 112 – *Paul und Paula*; zur Speicherung von Fernsehsendungen auf dem Server eines Anbeiters von Fernsehaufzeichungen vgl. OLG Dresden vom 28.11.2006, ZUM 2007, 203, 204; OLG Köln vom 09.09.2005, GRUR-RR 2006, 5; sowie OLG Dreseden vom 20.03.2007, ZUM-RD 2008, 6, 7; vgl. auch *Loewenheim*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 20, Rn. 14; *Loewenheim*, in: *Schricker* (Hrsg.), Urheberrecht, 2006, § 16, Rn. 22; *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, § 16 Rn. 7; *Dustmann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 16 UrhG Rn. 26.

1071 KG vom 24.07.2001, GRUR 2002, 252, 253 – *Mantellieferung*; *Schulze*, in: *Dreier/Schulze*, UrhG, 2008, § 16 Rn. 13; *Loewenheim*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 20, Rn. 14.

bb. Recht der öffentlichen Zugänglichmachung

Das Recht der öffentlichen Zugänglichmachung wurde durch den Ersten Korb der Urheberrechtsreform eingeführt, mit dem die Vorgaben der Multimediarichtlinie im UrhG umgesetzt wurden.[1072] Damit wurde klargestellt, dass auch die digitale Zurverfügungstellung von urheberrechtlich geschützten Werken dem Ausschließlichkeitsrecht des Urhebers unterfällt.[1073] Zwar war bereits vor Einführung dieses speziellen Rechts anerkannt, dass solche Handlungen vom Zuweisungsgehalt des an einem Werk bestehenden Urheberrechts erfasst werden. Allerdings war die rechtliche Einordnung dieses Rechts unter die bestehenden Ausschließlichkeitsrechte im Einzelnen umstritten.

§ 19 a UrhG ergänzt damit im Bereich der digitalen Datenübertragung das Verbreitungsrecht gem. § 17 UrhG. Denn dieses Verwertungsrecht erfasst nur Handlungen, durch das ein Werk der Öffentlichkeit durch die Verbreitung körperlicher Werkstücke zugänglich gemacht wird.[1074] Bei der Verbreitung von Werken im Wege der Datenfernübertragung handelt es sich jedoch nicht um eine Übermittlung körperlicher Gegenstände, weswegen die Übermittlung von Werken über das Internet in Form von digitalen Dateien von § 17 UrhG nicht erfasst wird.[1075] Ein urheberrechtlich geschütztes Werk wird im Sinne von § 19 a UrhG „drahtgebunden oder drahtlos der Öffentlichkeit ... zugänglich" gemacht, wenn für Mitglieder der Öffentlichkeit die abstrakte Möglichkeit besteht, auf das Werk zuzugreifen.[1076] Die Vorschrift bezieht sich somit auf das Bereithalten eines urheberrechtlich geschützten Werks zum Abruf durch die Öffentlichkeit.[1077] „Mitglieder der Öffentlichkeit" sind Personen, die weder mit demjenigen, der das Werk zugänglich gemacht hat, noch mit den anderen Personen, die ebenfalls auf das Werk zugreifen können, persönlich verbunden sind.[1078] Keine Rolle spielt in diesem Zusammenhang, wie der Zugriff auf das Werk in technologischer Hinsicht im Einzelnen abläuft.[1079] Weitere Voraussetzung ist, dass das Werk den Mitgliedern der Öffentlichkeit „von Orten

1072 Vgl. 4. Kapitel, Teil D.II.2.
1073 *Lauber/Schwipps*, GRUR 2004, 293, 294; *Schippan*, ZUM 2003, 378, 379.
1074 *Loewenheim*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 20, Rn. 21; *Dustmann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 17 Rn. 8; *Loewenheim*, in: *Schricker* (Hrsg.), UrhR, § 17, Rn. 4; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 19 a, Rn. 5.
1075 *Loewenheim*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010, § 20, Rn. 21; *Dustmann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 17 Rn. 9; *Loewenheim*, in: *Schricker* (Hrsg.), UrhR, § 17, Rn. 5.
1076 *Dustmann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 19 a UrhG Rn. 7; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 19 a, Rn. 6.
1077 *von Ungern-Sternberg*, in: *Schricker* (Hrsg.), UrhR, 2006, § 19 a, Rn. 42.
1078 Vgl. die Legaldefinition des Begriffs Öffentlichkeit gemäß § 15 Abs. 3 S. 2 UrhG.
1079 *Dustmann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 19 a UrhG Rn. 10 spricht von einer „technologieneutralen" Ausgestaltung des § 19 a UrhG; ebenso *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 19 a, Rn. 6.

und zu Zeiten ihrer Wahl" zugänglich ist. Mit dieser Formulierung wird zum einen klargestellt, dass § 19 a UrhG die sogenannte „sukzessive" Öffentlichkeit erfasst, für die nicht – wie etwa im Falle des Vorführungsrechts gemäß § 19 Abs. 4[1080] – erforderlich ist, dass ein Werk gleichzeitig von einer Mehrzahl Personen wahrgenommen wird.[1081] Zum anderen wird hierdurch der Anwendungsbereich von § 19 a UrhG von demjenigen der Rechte der Wahrnehmbarmachung (§§ 19, 21 und 22 UrhG) sowie des Senderechts (§ 20 UrhG) abgegrenzt.[1082] Ein Beispiel für einen Fall der öffentlichen Zugänglichmachung im Sinne von § 19 a UrhG ist die Verfügbarmachung urheberrechtlich geschützter Inhalte auf Webseiten im Internet.[1083] Auch fallen hierunter Streaming-Angebote,[1084] wodurch es dem Nutzer ermöglicht wird, das geschützte Werk zu Zeiten und Orten seiner Wahl zu konsumieren, ebenso wie die Konstellation, dass ein Nutzer im Rahmen von zentralen oder dezentralen Filesharing-Netzwerken auf seinem Computer digitale Werke für den öffentlichen Zugriff anderer Teilnehmer zur Verfügung stellt.[1085]

Wenn ein Nutzer eine Datei, die ein urheberrechtlich geschütztes Multimediawerk enthält, auf einen Web 2.0-Dienst hochlädt, so ist diese Datei – und damit auch das darin verkörperte Multimediawerk – ab diesem Zeitpunkt in der Regel ohne Einschränkung für alle weiteren Nutzer des Web 2.0-Dienstes abrufbar. Das bedeutet, dass ein unbeschränkter Personenkreis theoretisch zu jeder Zeit und von jedem Ort auf das Multimediawerk zugreifen kann, wobei der Zugriff lediglich von der Verfügbarkeit eines internetfähigen Computers abhängt. Damit ist eine öffentliche Zugänglichmachung im Sinne von § 19 a UrhG gegeben.

c. Passivlegitimation des Web 2.0-Dienstes bezüglich der Rechtsverletzungen der Nutzer

Der unmittelbare Eingriff in die dem Urheber vorbehaltenen Verwertungsrechte gemäß §§ 16, 19 a UrhG durch das Hochladen des Multimediawerks erfolgt im Rahmen von Web 2.0-Diensten in der Regel nicht durch den ISP selbst, sondern

1080 *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 19 Rn. 18.
1081 *Dustmann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 19 a UrhG Rn. 11; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 19 a, Rn. 10; *Lauber/Schwipps*, GRUR 2004, 293, 294.
1082 *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 19 a, Rn. 8.
1083 OLG Hamburg vom 28.04.2005, GRUR-RR 2005, 209, 211 – *Auskunftspflicht des Access Providers*; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 19 a, Rn. 6; *Dustmann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 19 a UrhG, Rn. 15.
1084 OLG Köln vom 09.09.2005, GRUR-RR 2006, 5 – *Personal Video Recorder*; OLG Hamburg vom 07.07.2005, MMR 2006, 173, 174 - *staytuned*; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 19 a, Rn. 6; *Dustmann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 19 a UrhG, Rn. 20.
1085 *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 19 a, Rn. 6; *Dustmann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 19 a UrhG, Rn. 18.

durch die Nutzer seines Internetdienstes. Es stellt sich die Frage, ob er ISP für ein solches Verhalten der Nutzer haftbar gemacht werden kann.

Der Anspruch aus § 97 Abs. 2 UrhG richtet sich gegen den denjenigen, der ein fremdes Urheberrecht verletzt. Dies ist grundsätzlich jeder, der die Rechtsverletzung als Täter selbst adäquat kausal begeht oder daran als Teilnehmer, d.h. als Anstifter oder Gehilfe, beteiligt ist.[1086] Hingegen haften bloße Hilfspersonen nicht für Urheberrechtsverletzungen Dritter.[1087] Als Teilnehmer ist derjenige zu qualifizieren, dem nach wertender Betrachtung die fremde unmittelbar rechtsverletzende Handlung wie eine eigene zugerechnet werden kann, da er sie veranlasst oder sich zu eigen gemacht hat.[1088] Dabei muss der Teilnehmer zumindest mit bedingtem Vorsatz – einschließlich dem Bewusstsein der Rechtswidrigkeit der Tat in ihrer konkreten Form – in Bezug auf die Haupttat gehandelt haben. [1089]

Die Beurteilung, ob jemand im Einzelfall als Teilnehmer der Urheberrechtsverletzung oder als bloße Hilfsperson anzusehen ist, hängt vor allem auch vom Tatbestand des jeweils betroffenen Verwertungsrechts ab.[1090] So ist Verletzer des Vervielfältigungsrechts gemäß § 16 UrhG grundsätzlich nur derjenige, der die Vervielfältigungshandlung selbst vornimmt.[1091] Lädt somit ein Nutzer ein urheberrechtlich geschütztes Multimediawerk auf einen Internetdienst hoch, so greift allein er hierdurch in das Vervielfältigungsrecht gemäß § 16 UrhG ein.[1092] Eine Zurechnung dieser Handlung an den ISP, auf dessen Server das Vervielfältigungsstück gespeichert wird, scheidet insoweit aus. Auch in Bezug auf das Recht der öffentlichen Zugänglichmachung gemäß § 19 a UrhG ist zuvorderst derjenige Täter, auf dessen Initiative und Verantwortung es zurückgeht, dass das Werk dem Zugriff der Öffentlichkeit ausgesetzt wird.[1093] Allerdings endet in diesem Fall die urheberrechtlich relevante Verwertungshandlung nicht mit Beendigung des technischen Vorgangs des Uploads, sondern besteht während des gesamten Zeitraums der Abrufbarkeit des geschützten Inhalts innerhalb des Dienstes des ISPs fort.[1094] Nach dem Vorgang des Hochladens gelangt das Multimediawerk jedoch in den

1086 *J.B. Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 97 UrhG, Rn. 145¸ *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 97, Rn. 23.
1087 *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 97, Rn. 32; *Wild*, in: *Schricker* (Hrsg.), UrhR, § 97, Rn. 38.
1088 *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 97, Rn. 23, 32; *J.B. Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 97, Rn. 148.
1089 BGH vom 11.03.2004, GRUR 2004, 860, 863/864 – *Internet-Versteigerung I*; *J.B. Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 97, UrhG, Rn. 153.
1090 *Dreier*, in: *Dreier/Schulze*, UrhG, 2008,§ 97, Rn. 23.
1091 *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 97 Rn. 28; *J.B. Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 97 UrhG, Rn. 149.
1092 *Hoeren*, in: *Sieber*/*Hoeren* (Hrsg.), Multimediarecht, 2010, 18.2 Rn. 74.
1093 *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 97, Rn. 30; *J.B. Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 97, Rn. 149.
1094 *Dustmann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 19 a, Rn. 9.

Organisations- und Kontrollbereich des ISPs und wird über dessen Internetdienst der Öffentlichkeit zugänglich gemacht. Daher ist insoweit auch der ISP für die Verletzung des Rechts aus § 19 a UrhG verantwortlich.[1095]

In Bezug auf die urheberrechtsverletzenden Handlungen, die Nutzer im Rahmen von Web 2.0-Diensten begehen, kommt somit eine Haftung des ISPs in erster Linie wegen der Verletzung des Rechts auf öffentliche Zugänglichmachung gemäß § 19 a UrhG in Betracht.

d. Die Haftungsbeschränkung gemäß § 10 TMG

Im Zusammenhang mit der Haftung von ISPs für Rechtsverletzungen, die innerhalb ihrer Internetdienste stattfinden, sind weiterhin die Haftungsbeschränkungen gemäß §§ 7-10 Telemediengesetz („TMG") zu beachten. Durch diese Bestimmungen werden die Voraussetzungen der Haftung von ISPs modifiziert und ihre Verantwortlichkeit in Bezug auf bestimmte Tätigkeiten eingeschränkt.[1096] § 10 TMG, der Art. 14 Abs. 1 der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt,[1097] auch E-Commerce-Richtlinie genannt (nachfolgend „ECRL"), in deutsches Recht umsetzt, beschränkt die Haftung von ISPs, deren Dienstleistung darin besteht, von Nutzern eingegebene Informationen im Auftrag der Nutzer zu speichern.[1098] Sie

1095 *Hoeren*, in: *Sieber*/*Hoeren* (Hrsg.), Multimediarecht, 2010, 18.2, Rn. 75; *Spindler*, in: Spindler/Schmitz/Geis, TDG, 2004, § 8, Rn. 14; a.A., wonach Host-Provider, die lediglich die technischen Mittel zum Abruf des Werks zur Verfügungs stellen, nicht eine Handlung im Sinne von § 19 a begehen, *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 19 a, Rn. 6; *von Ungern-Sternberg*, in: *Schricker* (Hrsg.), UrhR, 2006, Rn. 55; *Dustmann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 19 a UrhG, Rn. 27.

1096 *Spindler*, in: *Spindler/Schmitz/Geis*, TDG, 2004, Vor § 8 TDG Rn. 26; *Sobola/Kohl*, CR 2005, 443.

1097 Richtlinie 2000/31/EG vom 08.06.2000, ABl. EG Nr. L 178 v. 17.07.2000, S. 1; vgl. hierzu 8. Kapitel, Teil C.I.1.b.aa.(2.).

1098 Vgl. Art. 14 ECRL: *„(1) Die Mitgliedstaaten stellen sicher, dass im Fall eines Dienstes der Informationsgesellschaft, der in der Speicherung von durch einen Nutzer eingegebenen Informationen besteht, der Diensteanbieter nicht für die im Auftrag eines Nutzers gespeicherten Informationen verantwortlich ist, sofern folgende Voraussetzungen erfüllt sind:*
a) Der Anbieter hat keine tatsächliche Kenntnis von der rechtswidrigen Tätigkeit oder Information, und, in Bezug auf Schadenersatzansprüche, ist er sich auch keiner Tatsachen oder Umstände bewusst, aus denen die rechtswidrige Tätigkeit oder Information offensichtlich wird, oder
b) der Anbieter wird, sobald er diese Kenntnis oder dieses Bewusstsein erlangt, unverzüglich tätig, um die Information zu entfernen oder den Zugang zu ihr zu sperren.

stellt damit die Haftungsbeschränkung für Host-Provider dar und ist im deutschen Recht das Pendant zu der Safe-Harbor-Regelung gemäß 17 U.S.C. § 512(c).

aa. Entstehungsgeschichte

Die Regelungen gemäß §§ 7-10 TMG stellen das derzeitige Endergebnis jahrelanger Bemühungen dar, zunächst auf nationaler und seit Erlass der ECRL auch auf europäischer Ebene einen klaren und interessengerechten Rechtsrahmen betreffend die Haftung von ISPs für die Rechtsverletzungen der Nutzer ihrer Internetdienste zu schaffen.

(1) Das Teledienstegesetz von 1997

Die zunehmende Digitalisierung löste Mitte der 90'er Jahre in Deutschland eine Diskussion über notwendige Anpassungen der gesetzlichen Rahmenbedingungen für den sich rasant entwickelnden Markt internetbasierter Dienstleistungen aus. Der deutsche Gesetzgeber hielt es trotz der einfacheren Belangbarkeit von ISPs als „superior risk bearer"[1099] bald für unerlässlich, geeignete rechtliche Rahmenbedingungen für ISPs zu schaffen, um den Fortschritt auf dem Gebiet der elektronischen Kommunikation zu sichern.[1100] Vor diesem Hintergrund wurde das Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikations-

(2) Absatz 1 findet keine Anwendung, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.
(3) Dieser Artikel lässt die Möglichkeit unberührt, dass ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern, oder dass die Mitgliedstaaten Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs zu ihr festlegen.".

1099 Der „superior risk bearer" ist diejenige Partei innerhalb einer Vertragsbeziehung, die am Besten in der Lage ist, entweder die Wahrscheinlichkeit eines Schadenseintritts zu verringern, den aus der Nichtleistung (nonperformance) resultierenden Schadensumfang für den Betroffenen entweder noch vor (Vorbeugung) oder nach deren Eintritt (Schadensbegrenzung) zu minimieren oder sich (selbständig oder durch Dritte) gegen das Restrisiko des nicht vermeidbaren Schadens abzusichern. Es handelt sich hierbei um eine andere Bezeichung des „cheapest cost avoider", vgl. 8. Kapitel, Teil II.1.b.(bb)(5). Dies trifft im Kontext online begangener Rechtsverletzungen auf Host-Provider oftmals zu, da als Alternative nur die Inanspruchnahme des unmittelbaren Verletzers in Betracht kommt, der in der Regel nur schwer zu identifizeren ist und dessen Inanspruchnahme jedenfalls sehr viel zeitintensiver ist, als die Beseitigung des rechtswidrigen Zustands durch den Host-Provider, der insbesondere auch über die Kontrolle über die technische Infrastruktur des Internetdienstes verfügt; vgl. hierzu auch *Sieber*, CR 1997, 581; *Klatt*, ZUM 2009, 265, 270.

1100 *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1. Rn. 2; *Spindler*, in: *Spindler/Schmitz/Geis*, TDG, 2004, Vor § 8 TDG Rn. 2.

dienste (Informations- und Kommunikationsdienste-Gesetz – „IuKDG")[1101] erlassen, das in Artikel 1 IuKDG das sogenannte „Teledienstegesetz" („TDG 1997") enthielt. Das TDG 1997 trat gemeinsam mit fast[1102] allen anderen Regelungen des IuKDG am 01.08.1997 in Kraft. Ab diesem Zeitpunkt gehörte Deutschland zu den wenigen Staaten weltweit, die über ein speziell auf die Internetwirtschaft abgestimmtes, den „Lebenssachverhalt Multimedia" einheitlich umfassendes Regelungswerk verfügten,[1103] das in Form von § 5 TDG 1997 eine „pionierhafte" Regelung betreffend die Verantwortlichkeit von ISPs enthielt.[1104]

Streitigkeiten zwischen Bund und Ländern in Bezug auf die Gesetzgebungskompetenz für die neuen Medien führten dazu, dass parallel zum TDG 1997 von den Ländern der „Mediendienste-Staatsvertrag" („MDSt") beschlossen wurde.[1105] Dieser enthielt für an die Allgemeinheit gerichtete „Mediendienste"[1106] identische Regelungen wie das TDG 1997 für die der Individualkommunikation dienenden „Dienste der Informationsgesellschaft."[1107] In der Praxis gestaltete sich die Abgrenzung zwischen Medien- und Telediensten äußerst schwierig, war jedoch erforderlich, um die für einen Dienst jeweils zuständige Aufsichtsbehörde ermitteln zu können. Darüber hinaus konnten die auf Landesebene im MDStV geregelten Haftungsbeschränkungen für Mediendienste keine Wirkung in Bezug auf bundesrechtliche zivil-, urheber-, marken- oder wettbewerbsrechtliche Ansprüche zeitigen.[1108] Dadurch befanden sich die Anbieter von Mediendiensten haftungsrechtlich in einer wesentlich schlechteren Position als die Anbieter von Telediensten.

1101 Gesetz vom 13.06.1997, BGBl I 1997, S. 1870.

1102 Eine Ausnahme bildete lediglich Artikel 7 IuKDG (Änderung des Urheberrechts betreffend den rechtlichen Schutz von Datenbanken), der erst am 1.1.1998 in Kraft trat.

1103 *Engel-Flechsig/Maennel/Tettenborn*, NJW 1997, 2981; *Rossnagel*, NVwZ 2007, 743.

1104 *Hoeren*, NJW 2007, 801. Vgl. zur Rechtslage bezüglich der Haftung von ISPs unter § 5 TDG beispielsweise *Freytag*, Haftung im Netz, 1999; *Pankoke*, Von der Presse- zur Providerhaftung, 2000; *Sieber*, Verantwortlichkeit im Netz, 1999.

1105 *Rossnagel*, NVwZ 2007, 743; *Hoeren*, MMR 2007, 801; *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005, Teil D, Rn. 1.

1106 Vgl. § 2 Abs. 2 Nr. 4 MDStV.

1107 Vgl. § 2 TDG 1997. Maßgeblich für die Unterscheidung zwischen Mediendiensten und Telediensten war das Merkmal der redaktionellen Gestaltung zur Meinungsbildung für die Allgemeinheit, und somit die Frage, ob Gegenstand eines Internetdienstes sog. meinungsbildende, d.h. die allgemeine Diskussion betreffende weltanschauliche oder politische Inhalte waren. Traf dies zu, lag ein Mediendienst vor, anderenfalls handelte es sich um einen Teledienst. Demnach waren beispielsweise Meinungsforen, wenn die Einträge der Nutzer anbieterseitig durch einen Moderator bearbeitet oder zusammengestellt wurden, dem MDStV zuzuordnen. Hingegen galten Anbieter von E-Mail-Diensten oder Suchmaschinen in ihrer Eigenschaft als Dienste zur Ermöglichung individueller Kommunikation als Teledienste.

1108 *Hoeren*, in: *Hoeren/Sieber* (Hrsg.), *Multimediarecht, 2010*, 18.2 Rn. 65; s.a. *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005, Teil D, Rn. 2.

(2) Die E-Commerce-Richtlinie

Im Jahr 2000 wurde die Verantwortlichkeit von ISPs auf europäischer Ebene durch die ECRL harmonisiert. Ziel der ECRL war es, den freien Verkehr von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten sicherzustellen und zu fördern.[1109] Zur Erreichung dieses Ziels wurde die Schaffung von Rechtssicherheit für ISPs durch europaweit einheitliche Haftungsbeschränkungen als unerlässlich angesehen. Die Privilegierung von ISPs in Bezug auf die Rechtsverletzungen der Nutzer ihrer Internetdienste sah man aus zwei Gründen für gerechtfertigt an. Zum einen sollten ISPs ihre für den freien Informationsfluss im Internet und zur Fortentwicklung des elektronischen Geschäftsverkehrs notwendigen Dienstleistungen möglichst unbeeinträchtigt von rechtlichen Risiken erbringen können.[1110] Zum anderen hielt man eine effektive Kontrolle der riesigen Datenmengen, die die Server der ISPs tagtäglich passierten, praktisch nicht für möglich.[1111]

Die Beschränkung der Haftung von ISPs wurde in der ECRL in Art. 12 ff. geregelt. Die darin enthaltenen Vorgaben für die Mitgliedstaaten bezwecken eine Vollharmonisierung des Rechtsbereichs der Providerhaftung.[1112] Auf diese Weise sollte EU-weit ein einheitlicher Standard für die Haftung von ISPs geschaffen werden, um ein „race to the bottom" in Form eines Trends zur Niederlassung der ISPs in den EU-Ländern mit den mildesten Haftungsregeln zu verhindern.[1113] Die Mitgliedsstaaten dürfen somit bei der Umsetzung dieser Vorschriften in nationale Regelungen betreffend die Haftung von ISPs weder enger noch weiter fassen, als es die europarechtlichen Vorgaben vorsehen.[1114] Die Struktur der Verantwortlichkeitsregelungen gemäß Art 14 ff. ECRL wurde im Ergebnis weniger an die deutsche Regelung gemäß § 5 TDG 1997, sondern mehr an die US-amerikanische Safe-Harbor-Regelung gemäß 17 U.S.C. § 512 angelehnt.[1115] Die Haftung eines ISPs hängt dementsprechend von den bestehenden Kontroll- und Einflussmöglichkeiten auf einen technischen Vorgang und nicht von dessen inhaltlicher Nähe zu den je-

1109 Vgl. Art. 1 Abs. 1 ECRL; *Berger/Janal*, CR 2004, 917, 918.
1110 Vgl. KOM(2003) 702 endg., S. 14.
1111 *Tettenborn/Bender/Lübben/Karenfort*, BB-Beilage 10/2001, 1, 26.
1112 *Spindler*, in: *Spindler/Schmitz/Geis*, TDG, 2004, Vor § 8 TDG Rn. 3; *Berger/Janal*, CR 2004, 917, 918.
1113 *Tettenborn/Bender/Lübben/Karenfort*, BB-Beilage 10/2001, 1, 27.
1114 BT-Drs. 14/6098, S. 22; *Marly*, in: *Grabitz/Hilf/Nettesheim* (Hrsg.), EU, 2009, A 4, Art. 12, Rn. 3; *Heckmann*, in: *Heckmann*, jurisPK-Internetrecht, 2007, Vorbem. Kap. 1.7 Rn. 12; *Tettenborn/Bender/Lübben/Karenfort*, BB-Beilage 10/2001, 1, 27.
1115 BT-Drs. 14/6098, S. 22; *Marly*, in: *Grabitz/Hilf/Nettesheim* (Hrsg.), EU, 2009, A 4, Art. 12 Rn. 7; *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), *Multimediarecht, 2010*, 18.1 Rn. 4; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, Vor § 8 TDG Rn. 3; *Spindler*, NJW 2002, 921, 922; *Engels*, AfP 2000, 524, 529; *Freytag*, in: *Lehmann* (Hrsg.), Elektronic Business, 2002, Kap. F, Fn. 12.

weiligen Informationen ab.[1116] Dies geht insbesondere aus Erwägungsgrund 42 ECRL hervor, wonach die Haftungsbeschränkungen nur auf solche Tätigkeiten anwendbar sind, die „rein technischer, automatischer und passiver Art" sind, und zudem seitens des Providers „weder Kenntnis noch Kontrolle über die weitergeleitete oder gespeicherte Information" bestehen darf. Die Einschlägigkeit von Art. 12-14 ECRL in Bezug auf einen bestimmten Sachverhalt hängt somit von der Beschaffenheit der von dem ISP konkret erbrachten Tätigkeit ab und nicht davon, was für ein ISP (Accessprovider, Hostprovider, Suchmaschinenanbieter etc.) diese Leistung erbringt.[1117]

Als Ergänzung zu den Haftungsbeschränkungen schließt Art. 15 Abs. 1 ECRL[1118] die Möglichkeit aus, ISPs allgemein eine Verpflichtung zur Überwachung oder zur aktiven Durchsuchung der von ihnen übermittelten oder gespeicherten Informationen auf Umstände, die eine rechtswidrige Tätigkeit indizieren, aufzuerlegen. Mit diesem Ausschluss von Überwachungspflichten zulasten von ISPs verlieh der europäische Richtliniengeber seiner Überzeugung Ausdruck, dass eine systematische Überwachung ihrer Internetdienste für die ISPs praktisch unmöglich ist, weswegen die Auferlegung einer solchen Überwachungspflicht eine unverhältnismäßige Belastung für die ISPs darstellen würde.[1119] Außerdem wurde befürchtet, dass die Kosten einer solchen Überwachung im Ergebnis zu Lasten der Verbraucher gehen würden, in Form einer generellen Verteuerung des Zugangs zu Internetdiensten.[1120]

(3) Umsetzung der E-Commerce-Richtline in deutsches Recht durch das Teledienstegesetz von 2002 (seit 2007 Telemediengesetz)

Die ECRL wurde vom deutschen Gesetzgeber durch das Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz – „EGG")[1121] in nationales Recht umgesetzt. Artikel 1 EGG, der die Änderungen des TDG 1997 enthielt, trat am 1.1.2002 in Kraft („TDG

1116 *Sieber/Höfinger*, in: *Hoeren/Sieber*, Multimediarecht, 2010, 18.1 Rn. 17; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 8 Rn. 6; *Wiebe*, in: *Ernst/Vassilaki/Wiebe*, Hyperlinks, 2002, Rn. 137.

1117 *Marly*, in: *Grabitz/Hilf/Nettesheim* (Hrsg.), EU, 2009, A 4, Art. 12 Rn. 5; *Freytag*, CR 2000, 600, 605; *Tettenborn/Bender/Lübben/Karenfort*, BB-Beilage 10/2001, 1, 27.

1118 Vgl. Art. 15 Abs. 1 ECRL: *„Die Mitgliedstaaten erlegen Anbietern von Diensten im Sinne der Artikel 12, 13 und 14 keine allgemeine Verpflichtung auf, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen."*

1119 Vgl. KOM(2003) 702 endg., S. 16.

1120 s.o.

1121 Gesetz vom 14.12.2001, BGBl I 2001, S. 3721.

2002“).[1122] Die zu diesem Zeitpunkt bereits gemeinhin als unbefriedigend empfundene Doppelregelung der neuen Medien durch TDG und MDSt wurde durch das EGG nicht angetastet.[1123] Vielmehr wurden parallel zu den Haftungsregelungen des TDG auch diejenigen des MDStV novelliert.[1124] Im TDG 2002 waren die Haftungsregelungen für ISPs nunmehr in §§ 8-11 enthalten.

Mit Wirkung zum 01.03.2007 wurde das TDG 2002 durch das Telemediengesetz („TMG“) ersetzt, das als Artikel 1 des Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste („ElGVG“)[1125] verkündet wurde.[1126] Zeitgleich mit dem TMG trat der Neunte Rundfunkänderungsstaatsvertrag der Länder in Kraft, durch den der MDStV aufgehoben sowie der neue „Staatsvertrag für Rundfunk und Telemedien“ („RStV“) um ein Kapitel betreffend sogenannte „Telemedien“ ergänzt wurde.[1127] Durch die Einführung von TMG und RStV wurde die Verteilung der Zuständigkeit für Telemedien zwischen Bund und Ländern auf eine neue Grundlage gestellt. Demnach werden die wirtschaftlichen und datenschutzrechtlichen Aspekte der neuen Medien auf Bundesebene seither ausschließlich durch das TMG geregelt. Hingegen gelten für die materiellen Anforderungen betreffend presse- und rundfunknahe Medien die Regelungen in Abschnitt VI des RStV.[1128]

Im TMG wurden die Regelungen der §§ 8-11 TDG 2002 wortgleich in §§ 7-10 übernommen, obwohl eine umfassende Reform der Vorschriften zu diesem Zeitpunkt bereits vehement gefordert wurde.[1129] Hauptgrund für diese Forderungen war die Rechtsprechung des BGH zu Internetversteigerungen, durch die die Störerhaftung vom Anwendungsbereich der Haftungsbeschränkungen vollumfänglich ausgenommen und damit die Schutzwirkung dieser Bestimmungen zugunsten von ISPs erheblich eingeschränkt worden war.[1130] Trotzdem entschied sich der Gesetzgeber bei Einführung des TMG, in Bezug auf §§ 8-11 TDG 2002 keine Änderungen an der bestehenden Rechtslage vorzunehmen. Dies wurde vor allem mit dem Evaluierungsbericht der EU-Kommission zur ECRL begründet, der bis Ende 2007 veröffentlicht werden und sich unter anderem mit den Auswirkungen der auf EU-Ebene eingeführten Haftungsbeschränkungen für ISPs sowie dem insoweit gegebenenfalls bestehenden Handlungsbedarf befassen sollte. Dem wollte die

1122 Alle anderen Regelungen des EGG traten bereits am 21.12.01 in Kraft.
1123 *Hoeren*, NJW 2007, S. 801.
1124 *Sieber/Höfinger*: in *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, Multimediarecht 2010, 18.1 Rn. 3.
1125 Gesetz vom 26.02.2007, BGBl 2007 I, S. 179.
1126 *Roßnagel*, NVwZ 2007, 743.
1127 *Roßnagel* s.o.
1128 Vgl. § 1 Abs. 4 TMG; *Roßnagel*, NVwZ 2007, 743; *Hoeren*, NJW 2007, 802; *Spindler*, CR 2007, 239, 240.
1129 *Hoeren*, NJW 2007, 801, 805.
1130 Vgl. 8. Kapitel, Teil C.I.2.b.(aa).

Bundesregierung durch das TMG nicht vorgreifen.[1131] Allerdings lag der Evaluierungsbericht auch zum Zeitpunkt des Abschlusses der vorliegenden Arbeit immer noch nicht vor.

Da die Rechtsunsicherheit in diesem Bereich somit weiterhin groß ist,[1132] gab es im Jahr 2008 Bestrebungen der FDP, eine Novellierung des TMG anzustoßen, die allerdings zu keinem Ergebnis führten.[1133] Der Gesetzentwurf sah unter anderem vor, die Inanspruchnahme von ISPs betreffend die Entfernung oder Sperrung von rechtswidrigen Inhalten an die Voraussetzung zu knüpfen, dass entweder Maßnahmen gegen den verantwortlichen Nutzer nicht zielführend sind oder ein vollstreckbarer Titel gegen den verantwortlichen Nutzer vorliegt. [1134] Nach dem Wechsel in die Regierung hält die FDP gemeinsam mit dem Koalitionspartner CDU/CSU ausweislich des Koalitionsvertrages an ihrem Vorhaben der Novellierung des TMG fest.[1135] Im Juni 2010 lehnte dann jedoch die Justizminsterin Sabine Leutheusser-Schnarrenberger in ihrer „Berliner Rede zum Urheberrecht" eine gesetzliche Korrektur der Rechtsprechung des BGH grundsätzlich ab.[1136]

bb. Vereinbarkeit der Haftungsbeschränkungen mit höherrangigem Recht

Bereits zu Zeiten von § 5 TDG 1997 wurden teilweise Bedenken geäußert, dass in der Gewährung der Haftungsbeschränkungen zugunsten von ISPs ein Verstoß gegen das *Agreement on Trade-Related Aspects of Intellectual Property Rights* („TRIPS-Übereinkommen")[1137] liegen würde. Gemäß Art. 41, 45 TRIPS-Übereinkommen sind die Signatarstaaten verpflichtet, im Rahmen ihrer Rechtssysteme zu gewährleisten, dass im Falle einer Urheberrechtsverletzung ein Anspruch auf Schadensersatz geltend gemacht werden kann, wenn der Verletzer wusste oder vernünftigerweise hätte wissen können, dass er eine Verletzungshandlung begeht. Daraus wird abgeleitet, dass auch bei fahrlässig begangenen, mittelbaren Rechts-

1131 BT-Drs. 16/3078, S. 11 f.
1132 *Roßnagel*, NVwZ 2007, 743, 748.
1133 *Ohne Autor*, FDP fordert Reform der Haftungsregeln im Internet, Frankfurter Allgemeine Zeitung, 08.12.2008, S. 13.
1134 BT-Drs. 16/11173.
1135 CDU/CSU/FDP, Koalitionsvertrag, 2010, S. 103: *„Wir werden die Regelungen zur Verantwortlichkeit im Telemediengesetz fortentwickeln. Es gilt auch zukünftig einen fairen Ausgleich der berechtigten Interessen der Diensteanbieter, der Rechteinhaber und der Verbraucher zu gewährleisten."*
1136 Die Rede ist abrufbar unter http://www.bmj.bund.de/enid/0,41c20c636f6e5f6964092d0936393139093a095f7472636964092d0936393230/Reden/Sabine_Leutheusser-Schnarrenberger_1mt.html.
1137 Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums, BGBl. 1994 II S. 1730; das Übereinkommen ist als Anhang 1C des Übereinkommens zur Errichtung der Welthandelsorganisation am 1.1.1995 in Kraft getreten.

verletzungen eine Haftung eingreifen müsse.[1138] Diese Anforderung würde jedoch durch die ECRL unterlaufen, die gemäß Art. 14 Abs. 1 ECRL lediglich eine Haftung für evidente, d.h. grob fahrlässige Rechtsverstöße vorsehe und zudem in Art. 15 Abs. 1 ECRL aktive Überwachungs- und Nachforschungspflichten ausschließe.[1139] Dieser Rechtsauffassung widerspricht die überwiegende Meinung in der Literatur jedoch mit dem Argument, dass durch TRIPS lediglich die Haftungsvoraussetzungen für unmittelbare, nicht jedoch auch für mittelbare Urheberrechtsverletzungen geregelt werden sollten und es daher auf die Konstellation der Rechtsverstöße, die Art. 14 ECRL zum Gegenstand hat, keine Anwendung finden könne.[1140]

cc. Anwendbarkeit auf urheberrechtliche Ansprüche

Die Haftungsbeschränkungen gemäß §§ 8-10 TMG wirken im Falle ihrer Anwendbarkeit horizontal. Sie beschränken somit die zivil-, straf- und verwaltungsrechtliche Verantwortlichkeit von ISPs in Bezug auf sämtliche von Dritten im Rahmen der von ihnen betriebenen Internetdienste begangenen Rechtsverletzungen[1141] unabhängig davon, ob die jeweils einschlägige Haftungsnorm dem Bereich des Straf-, Zivil-, Verwaltungs- oder Jugendschutzrechts zuzuordnen ist. Weiterhin ist für ihre Anwendbarkeit unbeachtlich, ob die Haftung des ISPs von einem Verschulden abhängig ist.[1142] Dieser Querschnittcharakter der Vorschriften wird vor allem dem Begriff der „Verantwortlichkeit" entnommen, der bereits bei Einführung des TDG 1997 vom Gesetzgeber verwendet wurde, um den rechtsgebietsübergrei-

1138 *Lehmann*, CR 1998, 232, 233 f.; *ders*. ZUM 1999, 180, 184; *Schack*, MMR 2001, 9, 16.
1139 *Lehmann*, in: *Lehmann* (Hrsg.), Electronic Business, 2002, Kap. E Rn. 18.
1140 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, Vor § 8 TDG Rn. 5; *Dustmann*, Privilegierte Provider, 2001, 114 f.; *Sieber*, Verantwortlichkeit im Netz, 1999, Rn. 226; *Stadler*, Informationen im Internet, Rn. 56; *Marly*, in: *Grabitz/Hilf/Nettesheim* (Hrsg.), EU, 2009, A 4, Art. 14 Rn. 13; *Spindler*, MMR-Beilage 7/2000, 4, 21.
1141 *Spindler*, in: *Spindler/Schmitz/Geis*, TDG, 2004, Vor § 8 TDG Rn. 1; *Eck/Ruess*, MMR 2003, 363, 364; *Freytag,* in: *Lehmann* (Hrsg.), Electronic Business, 2002, Kap. F, Rn. 6. In Bezug auf Art. 12-14 ECRL vgl. KOM(2003) 702 endg., S. 14; *Marly*, in: *Grabitz/Hilf/Nettesheim* (Hrsg.), EU, 2009, A 4, Art. 12 Rn. 4; *Freytag*, CR 2000, 600, 604; *Spindler*, MMR-Beilage 7/2000, 4, 16; *ders*., NJW 2002, 921, 922; *Tettenborn/Bender/Lübben/Karenfort*, BB-Beilage 10/2001, 1, 27.
1142 *Roßnagel*, NVwZ 2007, 743, 747; *Sieber/Höfinger*, in: *Hoeren/Sieber*, 18.1 Rn. 15; *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005, Teil D, Rn. 9; *Spindler*, in: *Spindler/Schmitz/Geis*, TDG, 2004, Vor § 8 Rn. 13.

fenden Charakter der Haftungsbeschränkungen zu betonen.[1143] Hierunter ist generell das (Mit-)Einstehenmüssen für eine Rechtsverletzung zu verstehen.[1144]

Im Falle der Anwendbarkeit der Haftungsbeschränkung sind somit sämtliche zivilrechtliche Ansprüche auf Beseitigung, Unterlassung, Auskunft und Schadensersatz,[1145] und damit grundsätzlich auch urheberrechtliche Ansprüche, gegen den ISP ausgeschlossen.[1146] Die Anwendbarkeit der Haftungsbeschränkungen auch auf das Urheberrecht wird ausdrücklich belegt durch Erwägungsgrund 16 der Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft („InfoSoc-Richtlinie"),[1147] wonach die Haftungsbeschränkungen der ECRL – und damit die zu ihrer Umsetzung ergangenen deutschen Regelungen – die Haftung für Urheberrechtsverletzungen im Bereich des Internetverkehrs regeln.[1148] Weiterhin ergibt sich die Anwendbarkeit der Haftungsbeschränkungen auf das Urheberrecht auch aus dem TMG selbst. Dort ist in § 4 Abs. 4 Nr. 6 TMG geregelt, dass das Herkunftslandprinzip gemäß § 4 Abs. 1, 2 TMG auf das Urheberrecht keine Anwendung findet. Hieraus kann umgekehrt geschlossen werden, dass die sonstigen Vorschriften des TMG ohne Einschränkung auf das Urheberrecht anwendbar sind.[1149]

dd. Dogmatische Einordnung

Da § 10 TMG vorliegend im Zusammenhang mit einem möglichen urheberrechtlichen Schadensersatzanspruch geprüft wird, stellt sich die Frage nach der dogmatischen Einordnung der Haftungsbeschränkungen auf der Ebene des Tatbestands,

1143 BT-Drs. 13/7385, S. 20, 21; *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1 Rn. 15; *Hoeren,* in: *Hoeren/Sieber* (Hrsg.), *Multimediarecht, 2010*, 18.2 Rn. 105; s.a. *Spindler*, MMR 2001, 737; *Hoeren*, MMR 1998, 97 f. Zum „Querschnittscharakter" von § 5 TDG 1997 vgl. *Engels*, AfP 2000, 524, 526.

1144 *Freytag*, Haftung im Netz, 1999, S. 48; *ders*., CR 2000, 600, 604; *Engel-Flechsig/Maennel/Tettenborn*, NJW 1997, 2981, 2984.

1145 *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1 Rn. 15.

1146 *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005, Teil D, Rn. 5; mittlerweile unstreitig, a.A. noch (zu Zeiten von § 5 TDG) OLG München vom 08.03.2001, ZUM 2001, 420 – *Midi-Files*.

1147 Amtsblatt Nr. L 167 vom 22.06.2001, S. 10-19.

1148 Erwägungsgrund 16 InfoSoc-Richtlinie lautet: *„Die Haftung für Handlungen im Netzwerk-Umfeld betrifft nicht nur das Urheberrecht und die verwandten Schutzrechte, sondern auch andere Bereiche wie Verleumdung, irreführende Werbung, oder Verletzung von Warenzeichen, und wird horizontal in der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr") geregelt…."*

1149 *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005, Teil D, Rn. 15.

der Rechtswidrigkeit oder der Schuld. Diese Einordnung ist im Einzelnen umstritten.

Nach Vorstellung des Referentenentwurfs zum TDG 1997 sollte den damals in § 5 enthaltenen Haftungsbeschränkungen die Funktion zukommen, „dass ein möglicher Haftungsfall zunächst den Filter des § 5 passieren muss, bevor dann die Prüfung nach den Maßstäben des jeweiligen Rechtsgebiets ... erfolgen kann".[1150] Auch in der Begründung zum TDG 2002 heißt es insoweit, dass „... sich die Wirkungsweise der §§ 9 bis 11 untechnisch mit der eines Filters vergleichen" lässt. Daraus leitet sich die Vorfilter-Theorie ab, wonach die Haftungsbeschränkungen noch vor der Prüfung des Tatbestands der jeweils einschlägigen Haftungsnorm zu prüfen sind.[1151]

Literatur und Rechtsprechung gehen hingegen überwiegend davon aus, dass die Haftungsbeschränkungen als „tatbestandsintegrierter Vorfilter" einzuordnen sind.[1152] Für diese Auffassung spricht zum einen der Zweck der Haftungsbeschränkungen, die tatbestandliche Reichweite der jeweiligen strafrechtlichen und deliktischen Verbotsnorm von vornherein zu begrenzen.[1153] Durch sie wird festgelegt, ob und inwieweit ISPs, die im Rahmen ihrer Internetdienste sozialadäquate und im Interesse der Informationsgesellschaft liegende Leistungen erbringen, für das Verhalten Dritter im Zusammenhang mit diesen Leistungen einstehen müssen.[1154] Denn grundsätzlich handelt es sich bei der Informationsvermittlung um ein erlaubtes Risiko, aus dem sich keine negativen Haftungsfolgen ergeben.[1155] Weiterhin spricht für die Theorie des tatbestandsintegrierten Vorfilters, dass die Haftung eines ISPs für das rechtswidrige Verhalten seines Nutzers auch als Unterlassungshaftung eingeordnet werden kann. Demnach hängt die Haftung des ISPs davon ab, ob ihn eine Pflicht im Sinne einer strafrechtlichen Garanten- bzw. zivilrechtlichen Verkehrssicherungspflicht trifft, Maßnahmen zur Verhinderung des rechtswidri-

1150 Vgl. *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1 Rn. 14.

1151 *Engel-Flechsig/Maennel/Tettenborn*, NJW 1997, 2981, 2984; *Engel*, AfP 2000, 524, 526; *Köhler/Arndt/Fetzer*, Recht des Internet, 2008, Teil VII, Rn. 746. Diese Ansicht wird mit der Begründung abgelehnt, dass eine Verortung der Haftungsbeschränkungen außerhalb des Tatbestands zu Folgeproblemen hinsichtlich der persönlichen Haftung von Arbeitnehmern oder Organmitgliedern sowie in Bezug auf die akzessorische Haftung wegen Anstiftung oder Beihilfe führen würde, da sich die insoweit maßgeblichen Strukturen von Rechtswidrigkeit und Schuld nur auf den Tatbestand einer Haftungsnorm beziehen, vgl. *Spindler*, NJW 2002, 921, 922; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, Vor § 8 TDG ,Rn. 28.

1152 BGH vom 23.09.2003, CR 2004, 48, 49; *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1 Rn. 21 f.; *Buschle*, in: *Moritz/Dreier*, RHdB E-Commerce, 2005, Teil D, Rn. 272; *Freytag,* in: *Moritz/Dreier, RHdB E-Commerce, 2005,* Teil D, Rn. 144; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, Vor § 8 TDG Rn. 28..

1153 *Sieber/Höfinger* in *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1 Rn. 21.

1154 *Sieber/Höfinger* in *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1 Rn. 21; vgl. zur Sozialadäquanz von Providertätigkeiten gemäß §§ 8-10 TMG generell *Vassilaki*, MMR 2002, 659 ff.

1155 *Vassilaki*, MMR 2002, 659.

gen Verhaltens des Nutzers zu ergreifen. Insoweit wird durch die Haftungsbeschränkungen klargestellt, dass eine solche Pflicht eines ISPs, der Informationen im Internet übermittelt oder speichert, grundsätzlich ausscheidet bzw. nur unter bestimmten Bedingungen eingreift.[1156] Dies bedeutet, dass die aus einem Internetdienst resultierende allgemeine Betriebsgefahr grundsätzlich keine besonderen Pflichten des ISPs auslöst.[1157]

Folgt man somit der Theorie des tatbestandsintegrierten Vorfilters, ist das Nichteingreifen der Haftungsbeschränkungen gemäß §§ 8-11 TMG neben den eigentlichen Tatbestandsmerkmalen der jeweiligen Haftungsnorm quasi als negatives Tatbestandsmerkmal zusätzlich zu prüfen. Liegen die Voraussetzungen einer Haftungsbeschränkung im Falle eines ISPs vor, scheidet dessen Haftung im Ergebnis bereits auf Tatbestandsebene aus. Somit ist ein urheberrechtlicher Schadensersatzanspruch gegen einen Web 2.0-Dienst tatbestandlich ausgeschlossen, wenn dieser die Voraussetzungen der Haftungsbeschränkung gemäß § 10 TMG erfüllt.

ee. Die Tatbestandsvoraussetzungen der Haftungsbeschränkung für Host-Provider gemäß § 10 TMG

(1) Persönlicher Schutzbereich

Um die Haftungsbeschränkung für Host-Provider gemäß § 10 TMG beanspruchen zu können, muss ein Web 2.0-Dienst zunächst in den persönlichen Schutzbereich der Regelung fallen.

1156 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, Vor § 8 TDG Rn. 28.

1157 *Rücker*, CR 2005, 347, 348. Weiterhin spricht gegen die Einordnung der Haftungsbeschränkungen auf der Ebene der Rechtswidrigkeit oder der Schuld, dass hinter diesen Regelungen die Absicht steht, die Haftung von Host-Providern rechtsgebietsübergreifend „horizontal", d.h. einheitlich und objektiv zu beschränken, vgl. *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, Vor § 8 TDG Rn. 28. Eine Einordnung dieser Regelungen auf der Ebene der Rechtswidrigkeit würde jedoch bedeuten, dass das Verhalten des Providers zwar nicht rechtswidrig wäre, zunächst aber den Tatbestand einer Haftungsnorm erfüllen würde. Damit würde jedoch das Ziel nicht erreicht, Providertätigkeiten *a priori* als sozialadäquates, unwertfreies Verhalten zu qualifizieren. Die Einordnung als persönlicher Strafausschließungsgrund würde weiterhin bedeuten, dass die Haftungsbeschränkungen überhaupt nur bei verschuldensabhängigen Haftungsnomen zum Tragen kommen könnten. Dies würde Probleme in Bezug auf die Verantwortlichkeit von Teilnehmern sowie die rechtlichen Folgen von Irrtümern nach sich ziehen.

(i) Allgemeine Voraussetzungen

Die Haftungsbeschränkungen gemäß §§ 8-10 TMG finden auf „Diensteanbieter" im Sinne von § 2 S. 1 Ziff. 1 TMG Anwendung, d.h. auf jede natürliche oder juristische Person, „die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt."[1158] Telemedien sind gemäß § 1 Abs. 1 TMG alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 TKG, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG oder Rundfunk nach § 2 RStV darstellen.[1159] Von dieser Definition erfasst werden beispielsweise Meinungsforen, Weblogs, Newsgroups, Chatrooms, Datendienste, elektronische Bestelldienste, Handelsplattformen, Internetauktionsdienste, Suchmaschinen oder Email-Dienste.[1160] Diensteanbieter im Sinne von § 10 TMG sind somit natürliche oder juristische Personen, die die zuvor genannten elektronischen Informations- und Kommunikationsdienste entgeltlich oder unentgeltlich selbst betreiben oder den Zugang zu einem solchen Dienst vermitteln.

(ii) Eröffnung des persönlichen Schutzbereichs in Bezug auf Web 2.0-Dienste

Typische Web 2.0-Dienste sind soziale Netzwerke und Videoplattformen. Innerhalb solcher Internetdienste haben die Nutzer die Möglichkeit, Inhalte zu speichern und zu veröffentlichen sowie Nachrichten mit anderen Nutzern auszutauschen. Sie stellen daher eine Kombination weitgehend bekannter Funktionen von Email-Diensten, Meinungsforen und Weblogs dar. Da alle diese Dienste für sich genommen als „Diensteanbieter" im Sinne der gesetzlichen Definition gelten, ist auch

1158 Mit dieser Definition weicht das TMG von dem in der ECRL verwendeten Begriff der sogenannten „Dienste der Informationsgesellschaft" ab, worunter eine *„in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung"* zu verstehen ist. Aufgrund des Verzichts auf die Eingrenzung der Definition des TMG auf entgeltlich erbrachte Dienstleistungen geht der Anwendungsbereich des TMG weiter als derjenige der ECRL, indem auch private Tätigkeiten, die keinen kommerziellen Zwecken dienen, von ihm erfasst werden; vgl. *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1 Rn. 30; *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005, Teil D, Rn. 5; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, Vor § 8 TDG Rn. 21; sowie *Marly*, in: *Grabitz/Hilf/Nettesheim* (Hrsg.), EU, 2009, A 4, Art. 12 Rn. 6, der dafür eintritt, dass eine sachgerechte Auslegung des 4. Abschnittes der ECRL erfordert, diesen auch auf nicht-wirtschaftlich tätige Anbieter anzuwenden.

1159 *Roßnagel*, NVwZ 2007, S. 743, 744.

1160 *Heckmann,* in: *Heckmann,* jurisPK-Internetrecht, 2007, Vorbem. Kap. 1.7, Rn. 54 f.

davon auszugehen, dass Web 2.0-Dienste, die deren Funktionen teilweise auf sich vereinigen und neu kombinieren, ebenfalls Diensteanbieter darstellen.

(2) Sachlicher Schutzbereich

Weiterhin muss der Web 2.0-Dienst in den sachlichen Schutzbereich von § 10 TMG fallen.

(i) Allgemeine Voraussetzungen

Die Tätigkeit des Diensteanbieters muss darauf gerichtet sein, fremde Informationen für die Nutzer zu speichern. Denn § 10 TMG regelt das sogenannte „Hosting", worunter die öffentliche Zurverfügungstellung fremder Informationen auf eigenen oder zumindest selbst kontrollierten Servern verstanden wird.[1161]

Prägendes Merkmal der von § 10 TMG erfassten Dienstleistungen ist das Bereithalten von Speicher- und Rechnerkapazitäten zur Nutzung durch Dritte.[1162] Demnach muss der ISP eine technische Infrastruktur zur Verfügung stellen, innerhalb derer die Nutzer digitale Inhalte speichern und jederzeit abrufen können.[1163] Unerheblich ist insoweit, ob die gespeicherten Informationen außer für den Nutzer auch für Dritte zugänglich sind.[1164] Allerdings setzt § 10 TMG voraus, dass die Speicherung der Informationen von gewisser Dauer ist und die Informationen während des Zeitraums der Speicherung für den Nutzer beliebig abrufbar sind.[1165] Darüber hinaus ist jedoch nicht erforderlich, dass ein bestimmtes Rechtsverhältnis zwischen dem speichernden Nutzer und dem ISP besteht, da bereits die tatsächliche Veranlassung der Speicherung durch den Nutzer im System des ISPs zur Eröffnung des Schutzbereiches führt.[1166] Erforderlich ist, dass die Speicherung der Informationen auf die Veranlassung des Nutzers zurückgeht[1167] und der ISP an den Informationen keine Veränderungen vornimmt.[1168] Die Eigentumsverhältnisse an den vom ISP zur Speicherung genutzten Servern haben keinen Einfluss auf die Anwendbarkeit von § 10 TMG, solange der ISP die Funktionsherrschaft über die

1161 *Freytag,* in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005, Teil D, Rn. 121.
1162 *Heckmann*, in: *Heckmann*, jurisPK-Internetrecht, 2007, Vorbem. Kap. 1.7, Rn. 50.
1163 *Heckmann*, s.o.; *Sobola/Kohl*, CR 2005, 443, 444.
1164 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11 Rn. 5.
1165 *Spindler* s.o.
1166 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11 Rn. 7.
1167 *Heckmann*, in: *Heckmann*, jurisPK-Internetrecht, 2007, Vorbem. Kap. 1.10, Rn. 9; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11, Rn. 7.
1168 *Marly*, in: *Grabitz/Hilf/Nettesheim* (Hrsg.), EU, 2009, A 4, Art. 14, Rn. 9.

Server ausübt,[1169] d.h. die Informationen der Nutzer können durch den ISP entweder auf eigenen Servern gespeichert oder der benötigte Speicherplatz auf fremden Rechnern zur Verfügung gestellt werden.[1170]

§ 10 TMG erfasst somit so unterschiedliche Teledienste wie das Bereitstellen von Webseiten zur Nutzung durch Dritte, das Betreiben eines Schwarzen Bretts im Rahmen eines Usenets oder das Anbieten von Chatrooms, Auktionsplattformen oder Gästebüchern.[1171] Auch Videoplattformen und soziale Netzwerke unterfallen dem sachlichen Schutzbereich dieser Haftungsbeschränkung.[1172]

(ii) „Fremde" Informationen

Der ISP muss für den Nutzer „fremde Informationen" speichern. Der Begriff der Information wurde aus der ECRL in das TDG 2002/TMG übernommen. Er ersetzt den bis dahin verwendeten Begriff der „Inhalte". Der Intention des europäischen Richtliniengebers folgend ist der Begriff weit zu verstehen. Er umfasst sämtliche Angaben, die durch einen Teledienst übermittelt oder gespeichert werden können,[1173] d.h. kommunikative und nichtkommunikative Inhalte, die in digitalisierter Form in Computernetzen übertragen werden können.[1174]

Anders als Art. 14 ECRL, der sich seinem Regelungsgegenstand nach auf „vom Nutzer eingegebene" Informationen bezieht, erfordert § 10 TMG, dass die Informationen „fremd" sein müssen. Der Gesetzgeber hielt somit auch bei der Novellierung des TDG nach den Vorgaben der ECRL an der bereits im TDG 1997 eingeführten Unterscheidung zwischen „fremden" und „eigenen" Informationen fest. Aus der Gesetzesbegründung geht hervor, dass der Gesetzgeber mit der Beibehaltung dieser Begrifflichkeiten auch an der insoweit von der Rechtsprechung entwickelten Rechtsfigur der „zu eigen gemachten Information" festzuhalten beabsichtigte.[1175] Demnach können einem ISP Informationen, die von einem Dritten

1169 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11 Rn. 6; vgl. zum Meinungstand in Bezug auf die Frage der Eigentumsverhältnisse an den für einen Dienst genutzten Servern nach alter Rechtslage, d.h. zu Zeiten von § 5 TDG 1997 auch *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005, Teil D, Rn. 22.

1170 *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005, Teil D, Rn. 46.

1171 KOM(2003) 702 endg., Fn. 64; *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 79.

1172 *J.B. Nordemann*, in: Fromm/Nordemann (Hrsg.), UrhR, 2008, § 97 UrhG, Rn. 158; *Jürgens/Veigel*, AfP 2007, 181, 182; *Fülbier*, CR 2007, 515, 517.

1173 BT-Drs. 14/6098, S. 23.

1174 *Sieber/Höfinger* in *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 36; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, Vor § 8 TDG Rn. 23; *Heckmann,* in: *Heckmann*, jurisPK-Internetrecht, 2007, Vorbem. Kap. 1.7 Rn. 25; *Freytag,* in: *Lehmann (Hrsg.),* Electronic Business, 2002, Kap. F, Rn. 7.

1175 BT-Drs. 14/6098, S. 23; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 8 Rn. 5.

stammen und damit eigentlich „fremd" sind, dennoch als eigene zugerechnet werden, wenn sie sich aus Sicht eines verständigen Dritten als eigene Informationen des ISPs darstellen.[1176] Für die Beurteilung, ob in diesem Sinne eigene oder fremde Informationen vorliegen, ist maßgeblich, wie die Art und der Zweck der Übernahme der Informationen sowie ihre Präsentation durch den ISP im Rahmen seines Internetdienstes auf einen objektiven Beobachter wirken.[1177] Demnach kann das Vorliegen von „zu eigen gemachten" Informationen beispielsweise dann zu bejahen sein, wenn der ISP sich von in seinem Internetdienst vorhandenen rechtswidrigen Informationen nicht rechtzeitig distanziert.[1178] Für eigene Informationen haftet ein Provider gemäß § 7 Abs. 1 TMG ohne jede Einschränkung.

Aufgrund des Festhaltens an dieser Unterscheidung ist denkbar, dass nach deutschem Recht ein ISP entgegen der ECRL für „von einem Nutzer eingegebene" Informationen vollumfänglich haftet, wenn nach den von der Rechtsprechung entwickelten Grundsätzen davon auszugehen ist, dass der ISP sich diese Informationen zueigen gemacht hat. Dieses Ergebnis steht jedoch im Widerspruch zu Wortlaut und Zielsetzung von Art. 14 ECRL, wonach mit den Haftungsbeschränkungen bestimmte (technische) Tätigkeiten der ISPs, nicht jedoch bestimmte Arten von Informationen privilegiert werden sollten.[1179] Wie bereits erwähnt wurde, sollte maßgeblich für die Haftung eines ISPs gerade nicht die inhaltliche Nähe zu den Informationen sein, sondern die technischen Einwirkungsmöglichkeiten, die dem ISP in Bezug auf die Information zur Verfügung stehen. Zudem spricht auch das Verbot allgemeiner Überwachungspflichten zu Lasten von ISPs gemäß § 7 Abs. 1 S. 1 TMG[1180] gegen die Beibehaltung der Rechtsfigur der zu eigen gemachten Information. Denn nach den Grundsätzen der Rechtsprechung können fremde Informationen auch dann als durch den ISP angeeignet gelten, wenn dieser sich nicht rechtzeitig davon distanziert. Damit wäre jedoch ein ISP, der den Schutz von § 10 TMG für seine Tätigkeit sicherstellen will, gezwungen, die innerhalb seines Internetdienstes enthaltenen Informationen auf rechtswidriges Material hin zu durchsuchen, um sich rechtzeitig hiervon distanzieren zu können[1181] und unterläge damit faktisch einer allgemeinen Überwachungspflicht. Die fortgesetzte Anwendung der Rechtsfigur der zu eigen gemachten Information im Rahmen von §§ 8-10 TMG ist

1176 *Spindler* s.o.
1177 *Köhler/Arndt/Fetzer*, Recht des Internet, 2008, Teil VII, Rn. 748.
1178 BT-Drs. 14/6098, S. 23; vgl. *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005, Teil D, Rn. 17.
1179 KOM (2003) 702 endg., S. 14; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 8 Rn. 6.
1180 Vgl. 8. Kapitel, Teil C.I.b.ee.(3)(iv).
1181 *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 44.

daher als europarechtswidrig abzulehnen.[1182] Der Begriff „fremd" ist vielmehr unter Berücksichtigung der im Bereich der Haftungsbeschränkungen verbindlichen Vorgaben der ECRL[1183] so zu verstehen, dass darunter nurmehr von einem Nutzer eingegebene Informationen fallen.[1184]

(iii) Eröffnung des sachlichen Schutzbereichs in Bezug auf Web 2.0-Dienste

Das Charakteristikum von Web 2.0-Diensten besteht darin, über ihre Dienste den Nutzern die Speicherung eigener Inhalte im Internet zu ermöglichen. Daher fallen die Dienstleistungen von Web 2.0-Dienste grundsätzlich in den sachlichen Anwendungsbereich von § 10 TMG. Soweit sich diese Dienstleistungen der Web 2.0-Dienste auf „fremde" Informationen beziehen müssen, ist hierfür allein maßgeblich, dass es sich um „von den Nutzern eingegebene" Informationen handelt. Hingegen können insoweit die von der deutschen Rechtsprechung entwickelten Grundsätze über das Zueigenmachen fremder Informationen aufgrund der Vorgaben der ECRL keine Anwendung finden.

(3) Subjektive Ausschlusskriterien

Gemäß § 10 S. 1 Ziff. 1 Alt. 1 TMG ist Voraussetzung für das Eingreifen der Haftungsbeschränkung, dass der ISP „keine Kenntnis von der rechtswidrigen Handlung oder der Information" hat.

(i) Positive Kenntnis im Sinne von § 10 S. 1 Ziff. 1 Alt. 1 TMG

Unter Kenntnis in diesem Sinne ist nach der herrschenden Meinung tatsächliche, d.h. konkrete, auf eine bestimmte Information bezogene positive Kenntnis im Sinne

1182 *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 39; *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005, Teil D, Rn. 18; *Wiebe*, in: *Ernst/Vassilaki/Wiebe*, Hyperlinks, 2002, Rn. 143; *Köhler/Arndt/Fetzer*, Recht des Internet, 2008, Teil VII, Rn. 751; *Berger/Janal*, CR 2004, 917, 919; *Spindler*, NJW 2002, 921, 923. Allerdings wird diese Rechtsfigur insbesondere auch vom BGH weiterhin angewendet, vgl. z.B. BGH vom 12.11.2009, NJW-RR 2010, 1276 – *marions-kochbuch.de*. Mit dieser Argumentation hat daher z.B. das LG Hamburg die Anwendung von § 10 TMG auf die Internetplattform YouTube und damit auch die Anwendbarkeit des Verbots allgemeiner Überwachungspflichten gemäß § 7 Abs. 2 S. 1 TMG von vornherein verneint, mit dem Ergebnis, dass die Beklagte von dem Gericht uneingeschränkt als Störerin haftbar gemacht wurde, vgl. LG Hamburg vom 03.09.2010, BeckRS 2010, 21389.

1183 Vgl. 8. Kapitel, Teil C.I.1.b.aa.(2).

1184 *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 40.

von dolus directus zu verstehen.[1185] Damit wird die Haftung von ISPs auf vorsätzlich verwirklichte straf- und deliktsrechtliche Tatbestände beschränkt.[1186] Nicht ausreichend ist das Vorliegen von Fahrlässigkeit oder bedingtem Vorsatz (dolus eventualis),[1187] so dass beispielsweise allein der Umstand, dass der ISP weiß, dass das Auftreten von Rechtsverletzungen aufgrund der Beschaffenheit seines Internetdienstes nach der allgemeinen Lebenserfahrung zu erwarten ist, nicht zum Entfallen der Haftungsbeschränkung führt.[1188] Gleiches gilt für die Gleichsetzung von positiver Kenntnis mit fahrlässiger Unkenntnis im Sinne eines „Kennenmüssens"[1189] sowie die Annahme von normativer Kenntnis im Sinne eines bewussten Sichverschließens vor der Kenntnis von Rechtsverletzungen.[1190] Grund hierfür ist der eindeutige Wortlaut von § 10 TMG sowie der gesetzliche Ausschluss allgemeiner Überwachungspflichten gemäß § 7 Abs. 2 S. 1 TMG.[1191]

Zur Erfüllung von § 10 S. 1 Ziff. 1 Alt. 1 TMG reicht zudem nicht aus, dass aufgrund der Speicherung einer Information in dem vom ISP betriebenen System oder Netzwerk seitens des ISPs eine „abstrakte technische Kenntnis" diesbezüglich vorliegt.[1192] Erforderlich ist vielmehr „aktuelles menschliches Wissen".[1193] Allerdings gelten auch für die automatisierten Abläufe des Geschäftsbetriebs eines ISPs die allgemeinen Grundsätze über die Kenntniszurechnung innerhalb von Unternehmen. Dies bedeutet, dass ein ISP seine arbeitsteilige Organisation einschließlich der Prozesse zur elektronischen Datenverarbeitung nicht absichtlich so strukturieren darf, dass er von rechtswidrigen Informationen keine Kenntnis erhält. Denn

1185 Vgl. nur OLG München vom 17.05.2002, MMR 2002, 611, 612; LG Potsdam vom 10.10.2002, MMR 2002, 829; LG Düsseldorf MMR 2003, 120; *Sieber*/*Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 83; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, § 11 TDG Rn. 12; *Freytag,* in: *Lehmann* (Hrsg.), Electronic Business, 2002, Kap. F, Rn. 43; *Tettenborn/Bender/Lübben/Karenfort*, BB-Beilage 10/2001, 1, 31; *Marly*, in: *Grabitz/Hilf/Nettesheim* (Hrsg.), EU, 2009, A 4, Art. 14 Rn. 11.

1186 *Hoeren,* in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010*,* 18.2, Rn. 66.

1187 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, § 11 TDG Rn. 12; a.A. *Köhler/Arndt/Fetzer*, Recht des Internet, 2008, Teil VII, Rn. 767 ff.

1188 *Buschle*, in: *Moritz/Dreier*, RHdB E-Commerce, 2005, Teil D, Rn. 276; OLG München, GRUR 2001, 499.

1189 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11, Rn. 11.

1190 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11 Rn. 14; *Sieber*/*Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 83; *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, Teil D, Rn. 47; OLG Brandenburg vom 16.12.2003, MMR 2004, 330, 332; LG Düsseldorf vom 29.10.2002, MMR 2003, 120, 125; a.A. *Hoeren*, MMR 2004, 672, 673.

1191 Vgl. 8. Kapitel, Teil C.I.2.b.ee.(3)(iv): *Engels*, AfP 2000, 524, 528; a.A. *Klatt*, ZUM 2009, 265, 270.

1192 *Sieber*/*Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 83; *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005, Teil D, Rn. 47; *Köhler/Arndt/Fetzer*, Recht des Internet, 2008, Teil VII, Rn. 767 ff.

1193 LG Düsseldorf vom 29.10.2002, MMR 2003, 120; OLG Brandenburg vom 16.12.2003, MMR 2004, 330; *Sieber*/*Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 83.

dann trifft ihn gegebenenfalls ein Organisationsverschulden mit der Folge der Beweislastumkehr oder aber sogar der Vorwurf des rechtsmissbräuchlichen Verhaltens.[1194] Insoweit ist jedoch wiederum der Ausschluss allgemeiner Überwachungspflichten gemäß § 7 Abs. 2 S. 1 TMG zu beachten, weswegen Kenntnis nur im Falle eines evidenten Rechtsmissbrauchs, nicht jedoch bereits bei Vorliegen „nur" grober Mängel in der Organisationsstruktur des ISPs angenommen werden darf.[1195]

Der ISP hat aber jedenfalls dann positive Kenntnis im Sinne von § 10 S. 1 Ziff. 1 Alt. 1 TMG, wenn ihn ein Rechtsinhaber in Form einer schriftlichen und substantiierten Mitteilung auf eine konkrete Rechtsverletzung hinweist und der ISP hierdurch in die Lage versetzt wird, die Rechtsverletzung ohne großen personellen und finanziellen Aufwand aufzufinden.[1196] Der Erhalt einer Abmahnung führt somit regelmäßig zum Entfallen der Haftungsbeschränkung gemäß § 10 S. 1 Nr. 1 Alt. 1 TMG, es sei denn, der ISP beseitigt oder sperrt daraufhin die rechtswidrige Information unverzüglich.[1197]

(ii) Kenntnis auch der Rechtswidrigkeit?

Höchst umstritten war im Zusammenhang mit § 10 S. 1 Ziff. 1 Alt. 1 TMG, ob hierfür Kenntnis von der Information oder Handlung an sich ausreicht oder ob dem ISP darüber hinaus speziell auch deren Rechtswidrigkeit bekannt sein muss.

Aufgrund des eindeutigen Wortlauts von § 5 Abs. 2 TDG 1997, der die Rechtswidrigkeit mit keinem Wort erwähnte,[1198] war vor Einführung des TDG 2002 bzw. TMG allgemein anerkannt, dass für den Verlust des Schutzes der Haftungsbeschränkung nur Kenntnis des fraglichen Inhalts an sich, nicht jedoch auch der Rechtswidrigkeit dieses Inhalts erforderlich war.[1199] Insoweit war nach den im Presse- und Medienrecht allgemein gültigen Kriterien lediglich zu prüfen, ob der ISP seinen rechtlichen Kontrollpflichten Genüge getan hatte.[1200] Der Wortlaut von § 10 S. 1 Nr. 1 TMG[1201] lässt sich hingegen auch so verstehen, dass Voraussetzung

1194 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11 Rn. 27, 32; *Köhler/Arndt/Fetzer*, Recht des Internet, 2008, Teil VII, Rn. 771.
1195 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11 Rn. 22.
1196 *Köhler/Arndt/Fetzer*, Recht des Internet, 2008, Teil VII, Rn. 771.
1197 Vgl. 8. Kapitel, Teil C.I.1.d.ee.(4).
1198 *„Diensteanbieter sind für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann verantwortlich, wenn sie* von diesen Inhalten Kenntnis *haben"* (Hervorhebung durch die Verfasserin).
1199 *Neubauer* in *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005 Teil D, Rn. 22 a; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11 Rn. 17; *Engels*, AfP 2000, 524, 528; *Spindler*, MMR-Beilage 7/2000, 4, 18.
1200 *Spindler* s.o.
1201 *„...keine Kenntnis von der* rechtswidrigen *Handlung oder der Information"* (Hervorhebung durch die Verfasserin).

für das Entfallen der Haftungsbeschränkung auch positive Kenntnis von der Rechtswidrigkeit der Information oder Handlung seitens des ISPs ist.[1202] Aus der amtlichen Begründung zum TDG 2002 geht hervor, dass der deutsche Gesetzgeber die Vorgaben der ECRL diesbezüglich so verstanden hatte, dass im Falle einer rechtswidrigen Information allein die Kenntnis von deren Existenz, im Falle einer rechtswidrigen Handlung jedoch zudem die Kenntnis von deren Rechtswidrigkeit seitens des ISPs vorliegen müsse.[1203] Diese Differenzierung wurde von der Literatur jedoch überwiegend mit der Begründung abgelehnt, dass sie keine Stütze in Art. 14 ECRL finde.[1204]

Da somit der genaue Bezugspunkt des Kenntniserfordernisses aus dem Gesetz selbst nicht klar hervorgeht und zudem die Gesetzesbegründung insoweit keine überzeugende Klarstellung enthält, wurde einerseits argumentiert, dass im Rahmen von § 10 TMG generell die Kenntnis auch der Rechtswidrigkeit einer Information oder Handlung erforderlich sei. Dies wurde damit begründet, dass es im Internet oftmals schwierig sei, Rechtsverstöße als solche zu identifizieren.[1205] Außerdem sei die Hinzufügung des Attributs „rechtswidrig" in den Wortlaut der Regelung ansonsten überflüssig.[1206] Schließlich gehe aus der Begründung der Kommission zum ersten Richtlinienvorschlag hervor, dass diese in der Kenntnis von einer Rechtsverletzung – und damit der Rechtswidrigkeit einer Information oder Handlung – die Grundlage für die Haftung von ISPs sehe.[1207] Die Kenntnis auch der Rechtswidrigkeit sei somit erforderlich, auch wenn dies bedeute, dass dadurch im Ergebnis rechtsunkundige ISPs belohnt und die Grundsätze über den Verbotsirrtum in Frage gestellt würden.[1208] Diese Rechtsansicht wurde nunmehr höchstrichterlich durch den EuGH in seiner Entscheidung vom 23.03.2010 bestätigt.[1209] Darin hält das Gericht ausdrücklich fest, dass ein Anbieter für Daten, die er für einen Nutzer

1202 *Eck/Ruess*, MMR 2003, 363, 364.

1203 BT-Drs. 14/6098, S. 25. Inhaltlich begründet wurde diese Unterscheidung damit, dass, wenn eine Information wie beispielsweise eine volksverhetzende Nachricht bereits „als solche" zu beanstanden sei, der ISP seine Schutzwürdigkeit bereits in dem Zeitpunkt verliere, in dem er von der Existenz dieser Information Kenntnis erlange. Sei hingegen erst die in Bezug auf eine Information vorgenommene Handlung rechtswidrig, könne dies von Außenstehenden regelmäßig kaum erkannt werden und müsse der Verlust des Schutzes der Haftungsbeschränkung daher zusätzlich davon abhängig sein, dass dem ISP gerade auch diese Rechtswidrigkeit bekannt gewesen sei.

1204 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11 Rn. 19; *Sobola/Kohl*, CR 2005, 443, 447; *Eck/Ruess*, MMR 2003, 363, 365; *Tettenborn/Bender/Lübben/Karenfort*, Beilage BB 10/2001, 1, 32; a.A. *Gerke*, MMR 2003, 602, 603; *Marly*, in: *Grabitz/Hilf/Nettesheim* (Hrsg.), EU, 2009, A 4 Art. 15 Rn. 12; *Köhler/Arndt/Fetzer*, Recht des Internet, 2008, Teil VII, Rn. 765.

1205 *Hoeren,* in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010*,* 18.2 Rn. 68.

1206 *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005 Teil D, Rn. 47 b.

1207 KOM(1998)586, S. 32.

1208 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11 Rn. 20; *Spindler*, NJW 2002, 921, 924.

1209 EuGH vom 23.03.2010, Rs. C-236/08 bis C 238/08, Google France/Louis Vuitton.

gespeichert hat, gem. Art. 14 ECRL nicht zur Verantwortung gezogen werden kann, „es sei denn, er hat die Informationen nicht unverzüglich entfernt oder den Zugang zu ihnen gesperrt, nachdem er *von der Rechtswidrigkeit* dieser Informationen oder Tätigkeiten … *Kenntnis erlangt* hat."[1210] Die vom EuGH postulierte Erforderlichkeit der Kenntnis gerade auch der Rechtswidrigkeit einer Information oder Handlung wurde auch bereits vom BGH in seiner Entscheidung vom 29.04.2010[1211] zu Kenntnis genommen und bestätigt. Insoweit heißt es in der Urteilsbegründung, dass nach der vorgenannten Entscheidung des EuGH eine Haftung des beklagten Suchmaschinenbetreibers erst dann in Betracht kommt, „wenn er *von der Rechtswidrigkeit* der von ihm gespeicherten Information *Kenntnis erlangt* hat. Ein solcher die Haftung auslösender Hinweis auf eine Urheberrechtsverletzung muss ihm [dem Suchmaschinenbetreiber] auch über die urheberrechtliche Berechtigung der Beteiligten hinreichende Klarheit verschaffen."[1212]

Als Ergebnis ist somit festzuhalten, dass sich das Kenntniserfordernis gemäß § 10 S. 1 Ziff. 1 Alt. 1 TMG nicht nur auf die Existenz, sondern auch auf die Rechtswidrigkeit der Information oder Handlung bezieht.[1213]

(iii) Grob fahrlässige Unkenntnis gemäß § 10 S. 1 Nr. 1 Alt. 2 TMG

In Bezug auf Schadensersatzansprüche geht der Schutz der Haftungsbeschränkung gemäß § 10 S. 1 Nr. 1 2. Alt. TMG bereits dann verloren, wenn dem ISP „Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird." Es wird somit die Kenntnis, die zum Entfallen der Haftungsbeschränkung führt, auf die Begleitumstände einer Rechtsverletzung vorverlagert[1214] und somit der ISP im Falle von Schadensersatzansprüchen bereits bei Vorliegen von Unkenntnis von einer Rechtsverletzung, die durch grobe Fahrlässigkeit verursacht wurde, vom Schutz der Haftungsbeschränkung ausgeschlossen.[1215] Es muss sich jedoch um eine bewusste grobe Fahrlässigkeit handeln, die

1210 EuGH vom 23.03.2010, Rs. C-236/08 bis C 238/08,Tz. 120 (Hervorhebung durch die Verfasserin).
1211 BGH vom 29.04.2010, I ZR 69/08 – *Vorschaubilder*.
1212 BGH vom 29.04.2010, I ZR 69/08, Rz. 39 (Hervorhebung durch die Verfasserin).
1213 So auch *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, Teil 18.1, Rn. 84 ff.; a.A. *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, § 11 TDG Rn. 19; *Sobola/Kohl*, CR 2005, 443, 447; *Eck/Ruess*, MMR 2003, 363, 365; *Freytag*, CR 2000, 600, 608; *Dustmann,* Privilegierte Provider, 2001, 107.
1214 *Spindler*, MMR 2001, 737, 741.
1215 *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 90; *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005, Teil D, Rn. 51; *Tettenborn/Bender/Lübben/Karenfort*, BB-Beilage 10/2001, 1, 32; *Spindler*, MMR-Beilage 7/2000, 4, 18; *Freytag,* in: *Lehmann* (Hrsg.), Electronic Business, 2002, Kap. F, Rn. 43.

regelmäßig nur in klaren Evidenzfällen gegeben ist,[1216] d.h. in Fällen, in denen konkrete Hinweise auf die Begehung bestimmter rechtswidriger Handlungen oder die Existenz bestimmter rechtswidriger Inhalte vorliegen.[1217] Wenn somit ein ISP die Schadensersatzhaftung vermeiden will, trifft ihn bereits dann eine Handlungspflicht, wenn ihm Umstände bekannt werden, die auf eine offensichtliche Rechtsverletzung hinweisen.

(iv) Der Ausschluss allgemeiner Überwachungspflichten gemäß § 7 Abs. 2 S. 1 TMG

Gemäß § 7 Abs. 2 S. 1 TMG sind ISPs grundsätzlich nicht verpflichtet, die im Rahmen ihrer Dienste übermittelten bzw. gespeicherten Informationen zu überwachen oder auf Umstände zu durchsuchen, die das Vorliegen eines rechtswidrigen Inhalts oder rechtswidrigen Verhaltens indizieren.

§ 7 Abs. 2 S. 1 TMG setzt den Ausschluss allgemeiner Überwachungspflichten gemäß Art. 15 Abs. 1 ECRL in deutsches Recht um. Art. 15 ECRL ist als Ausdruck der grundsätzlichen Entscheidung des europäischen Richtliniengebers zu verstehen, wonach reguläre Tätigkeiten von ISPs nicht als besondere Gefahrenquellen, sondern als grundsätzlich sozialadäquates Verhalten anzusehen sind, aus dem daher auch keine erhöhten Sorgfaltsanforderungen resultieren.[1218] Zudem ist die Regelung das Ergebnis der zum Zeitpunkt des Erlasses der ECRL vorherrschenden Überzeugung, dass ISPs, die lediglich als neutrale Vermittler von Informationen fungieren, faktisch nicht dazu in der Lage sind, den gesamten von ihnen übermittelten oder gespeicherten Datenverkehr zu kontrollieren.[1219] Da somit eine effektive Kontrolle ohnehin als ausgeschlossen galt, sollte gesetzlich sichergestellt werden, dass den ISPs von den Gerichten keine sinnlosen „arbeits- und kontrollaufwändigen Überwachungsverpflichtungen“[1220] auferlegt werden würden.

Entsprechend dieser Vorgabe können ISPs nur zu konkreten reaktiven, nicht aber zu generellen präventiven Überwachungsmaßnahmen verpflichtet werden.[1221] Eine generell-präventive Überwachungspflicht liegt vor, wenn ein ISP gezwungen wird, sich vorbeugend von sämtlichen im Rahmen des von ihm angebotenen Internetdienstes übermittelten oder gespeicherten Daten, von denen er im

1216 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11 Rn. 23; *Stadler*, Informationen im Internet, Rn. 279 f.; *Eck/Ruess*, MMR 2003, 363, 364.
1217 LG Düsseldorf vom 29.10.2002, MMR 2003, 120.
1218 *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 53; *Rücker*, CR 2005, 347, 348.
1219 Erwägungsgrund 42 ECRL; *Tettenborn/Bender/Lübben/Karenfort*, BB-Beilage 10/2001, 1, 26, 33; *Rücker*, CR 2005, 347, 348.
1220 KOM(2003)702 endg. S. 22.
1221 *Hoeren,* in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010*,* 18.2, Rn. 102.

normalen Betrieb regelmäßig keine Kenntnis nehmen würde, Kenntnis zu verschaffen und sie auf ihre mögliche Rechtswidrigkeit hin zu überprüfen.[1222] Proaktive Kontrollpflichten bestehend in der „menschlichen Kenntnisnahme"[1223] einzelner, unspezifischer Informationen sind somit unzulässig. Hingegen liegt eine konkret-reaktive Überwachungspflicht vor, wenn ein ISP seinen Dienst zum Zwecke der Beseitigung oder Verhinderung einer Rechtsverletzung im Zusammenhang mit einer konkreten bekannten bzw. aus den Umständen offensichtlichen Information überwachen muss.[1224] Solche anlassbezogenen Überwachungsmaßnahmen bleiben weiterhin zulässig.[1225]

Der Ausschluss allgemeiner Überwachungspflichten wirkt sich insbesondere auf die Auslegung von § 10 S. 1 Ziff. 1 Alt. 1 TMG aus, wonach die Haftungsbeschränkung nicht anwendbar ist, wenn seitens des ISPs grob fahrlässige Unkenntnis von offensichtlichen Rechtsverstößen vorliegt. Dieser subjektive Haftungsmaßstab darf wegen § 7 Abs. 2 S. 1 TMG nicht als durch einen ISP erfüllt angesehen werden, wenn dieser seinen Dienst nicht aktiv nach Rechtsverletzungen durchsucht.[1226] Vielmehr ist der ISP im Rahmen von § 10 S. 1 Ziff. 1 Alt. 1 TMG lediglich dazu verpflichtet, ihm *bereits bekannte* Umstände daraufhin zu überprüfen, ob sich daraus die Existenz einer evidenten Rechtsverletzung ergibt.[1227] Diese Umstände müssen weiterhin so präzise sein, dass der ISP die rechtswidrigen Informationen ohne großen Aufwand auffinden und prüfen kann.[1228] Denn anderenfalls würde der ISP wiederum faktisch zu einer allgemeinen Überwachung seines Internetdienstes gezwungen.[1229]

1222 *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 54.
1223 *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 61.
1224 *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 54.
1225 S.o.
1226 *Spindler*, MMR-Beilage 7/2000, 4, 18.
1227 *Spindler*, MMR 2001, 737, 741.
1228 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11 Rn. 22.
1229 Ähnlich auch *Eck/Ruess*, MMR 2003, 363, 365; *Sobola/Kohl*, CR 2005, 443, 447; *Spindler*, NJW 2002, 921, 924, die allerdings sämtlich von der Erforderlichkeit auch der Kenntnis der Rechtswidrigkeit im Rahmen von § 10 S. 1 Ziff. 1 Alt. 1 TMG ausgehen, und daher wegen des Verbotes allgemeiner Überwachnungspflichten in Bezug auf § 10 S. 1 Ziff. 1 Alt. 1 TMG davon ausgehen, dass sich die grob fahrlässige Unkenntnis des Host-Providers nur auf die Unkenntnis von der Rechtswidrigkeit einer bereits bekannten Information oder Handlung, nicht hingegen auf die Existenz der Handlung oder Information an sich beziehen kann.

(v) Auswirkungen von Content-Identification-Technologien auf das Vorliegen der subjektiven Voraussetzungen in Bezug auf Web 2.0-Dienste

Zu prüfen ist, ob und inwieweit sich der Einsatz von Content-Identification-Technologien durch einen Web 2.0-Dienst auf das Vorliegen der subjektiven Voraussetzungen gemäß § 10 S. 1 Nr. 1, die zu einem Verlust der Haftungsbeschränkung führen können, auswirkt.

Gemäß § 10 S. 1 Nr. 1 1. Alt TMG verliert ein ISP den Schutz der Haftungsbeschränkung nur dann, wenn seinerseits positive Kenntnis im Sinne eines aktuellen, menschlichen Wissens von dem Vorhandensein einer rechtswidrigen Handlung oder von bestimmtem rechtswidrigem Material innerhalb seines Internetdienstes gegeben ist. Der Zweck einer Content-Identification-Technologie besteht jedoch nicht darin, dem ISP „aktuelle, menschliche" Kenntnis im Sinne von § 10 S. 1 Nr. 1 1. Alt TMG von den innerhalb seines Internetdienstes vorhandenen Inhalten zu verschaffen. Vielmehr wird lediglich als rechtswidrig identifiziertes Material im Rahmen eines automatisierten Prozesses von vornherein aussortiert, ohne dass der ISP dieses Material überhaupt jemals in irgendeiner Weise zur Kenntnis nehmen muss. Dies bedeutet jedoch, dass der Einsatz einer Content-Identification-Technologie dem ISP keine positive Kenntnis von dem hierdurch ausgefilterten rechtswidrigen Material verschafft. Da zudem auch ein absichtliches Sichverschließen vor der Kenntnis von einer Rechtsverletzung, wie es in dem bewussten Nichteinsatz von Content-Identification-Technologien zum Ausdruck kommen könnte, nicht mit positiver Kenntnis gleichgesetzt werden kann, wirkt sich im Rahmen von § 10 S. 1 Nr. 1 1. Alt TMG weder der Einsatz von Content-Identification-Technologien noch der bewusste Verzicht hierauf aus.

In Bezug auf Schadensersatzansprüche reicht gemäß § 10 S. 1 Nr. 1 Alt. 2 TMG für das Entfallen der Haftungsbeschränkung jedoch aus, dass dem ISP das Vorliegen einer Rechtsverletzung aufgrund grober Fahrlässigkeit, d.h. trotz der Kenntnis des ISPs von Umständen, die auf das Vorliegen einer Rechtsverletzung offensichtlich hinweisen, unbekannt geblieben ist. Fraglich ist, ob für ein grob fahrlässiges Verhalten in diesem Sinne die abstrakte Möglichkeit ausreicht, dass der ISP innerhalb seines Internetdienstes eine Content-Identification-Technologie einsetzen und auf diese Weise rechtswidriges Material identifizieren hätte können. Gegen eine solche Auslegung von § 10 S. 1 Nr. 1 Alt. 2 TMG spricht jedoch, wie dargelegt wurde, dass sich die Sorgfaltspflicht nur auf solche Umstände bezieht, die dem ISP bereits bekannt sind, d.h. keinerlei Verpflichtung des ISPs besteht, sich von unbekannten Umständen Kenntnis zu verschaffen und sie auf ihre Rechtswidrigkeit zu überprüfen. Damit besteht jedoch auch keine Verpflichtung, eine Content-Identification-Technologie einzusetzen, die dem ISPs grundsätzlich unbekannte Inhalte auf die urheberrechtliche Zulässigkeit hin überprüft.

Zudem steht einer solchen Ausdehnung des Sorgfaltsmaßstabes des ISPs der Ausschluss allgemeiner Überwachungspflichten gemäß § 7 Abs. 2 S. 1 TMG entgegen.[1230] Denn wenn aufgrund des Nichteinsatzes von Content-Identification-Technologien die subjektiven Anforderungen für den Ausschluss von § 10 TMG als erfüllt angesehen würden, wäre ein ISP faktisch dazu gezwungen, solche Technologien einzusetzen, wenn er den Schutz der Haftungsbeschränkung für sich sicherstellen will. Damit würde er jedoch gleichzeitig verpflichtet, seinen Internetdienst mit Hilfe dieser Technologien auf Rechtsverletzungen hin zu durchsuchen und somit in Bezug auf rechtswidriges Verhalten zu überwachen, d.h. läge eine präventiv-generelle Überwachungspflicht des ISPs vor, die dem Ausschluss allgemeiner Überwachungspflichten diametral entgegenlaufen würde.

Dieses Ergebnis wird durch die Entstehungsgeschichte der ECRL bestätigt.[1231] Denn eine Änderung, die das Europäische Parlament nach Vorlage des ersten Entwurfs der ECRL anregte, sah vor, den Einsatz technisch möglicher und zumutbarer Maßnahmen, deren Zweck in der präventiven Verhinderung der Nutzung rechtswidrig angebotener Inhalte besteht, von dem Verbot allgemeiner Überwachungspflichten auszunehmen.[1232] Dies wurde von der Europäischen Kommission jedoch mit der Begründung abgelehnt, dass hierdurch „in die Ausgewogenheit der Interessenabwägung“ eingegriffen würde.[1233] Diese Ablehnung der Europäischen Kommission dürfte auch auf der Erwägung beruht haben, dass im Zeitpunkt des Erlasses der ECRL im Jahr 2001 keine Technologien bekannt waren, mit denen ein solches Schutzniveau hätte erreicht werden können. Dies wird wiederum durch eine zwei Jahre später ergangene Stellungnahme der Kommission bestätigt, in der es heißt, „dass es den Berichten und Studien über die Wirksamkeit von Sperr- und Filteranwendungen zufolge noch keine Technik gibt, die nicht umgangen werden könnte und absolut wirksam unerlaubte und schädliche Informationen blockiert und filtert… .“[1234]

Als Ergebnis bleibt somit festzuhalten, dass sich auf das Vorliegen der subjektiven Ausschlusskriterien gemäß § 10 S. 1 Nr. 1 TMG weder der Einsatz von Content-Identification-Technologien noch der bewusste Verzicht hierauf zugunsten oder zulasten eines Web 2.0-Dienstes auswirkt.

1230 Vgl. 8. Kapitel, Teil C.I.1.d.ee.(3)(iv).
1231 *Rücker*, CR 2005, 347, 353.
1232 Vgl. Änderungsvorschlag 54 des Parlaments, Abl. EG Nr. C 279 v. 1.10. 1999, S. 389 ff.
1233 Vgl. Geänderter Richtlinienvorschlag der Kommission vom 17. 8.1999, KOM(1999) 427 endg., S. 8.
1234 Vgl. KOM(2003) 702 endg., S. 16; a.A. *Rössl/Rössl*, CR 2005, 809, 815, die vermuten, dass sich der Änderungsvorschlag lediglich auf technische Maßnahmen zu Zwecken der Strafverfolgung bezog.

(4) Unverzügliches Tätigwerden nach Kenntniserlangung

Gemäß § 10 S. 1 Nr. 2 TMG muss ein ISP, sobald er Kenntnis in Bezug auf eine Rechtsverletzung im Sinne von § 10 S. 1 Nr. 1 TMG erlangt hat, daraufhin unverzüglich Maßnahmen zur Beseitigung oder Sperrung der Information ergreifen, um den Schutz der Haftungsbeschränkung weiterhin für sich beanspruchen zu können. Nach Kenntniserlangung ist ein ISP somit verpflichtet, den Zugang Dritter zu der als rechtswidrig identifizierten Information effektiv und unverzüglich zu unterbinden.[1235] Unter dem Begriff „unverzüglich" ist ein Handeln ohne schuldhaftes Zögern zu verstehen.[1236] In diesem Zusammenhang kommen Verschuldenselemente einschließlich Zumutbarkeitserwägungen zum Tragen,[1237] so dass die Entfernung oder Sperrung einer Information nur im Rahmen des technisch Möglichen und Zumutbaren von dem ISP verlangt werden kann.[1238] Die Prüfung dieser Voraussetzungen erfordert somit eine Abwägung der sich im Einzelfall gegenüberstehenden Rechtsgüter.[1239] Zudem muss der ISP neben der technischen auch über die rechtliche Möglichkeit verfügen, die Information zu blockieren. Hierfür reicht jedoch bereits aus, dass der ISP die abstrakte Möglichkeit hat, sich die Berechtigung zur Sperrung oder Entfernung von Informationen in den allgemeinen Nutzungsbedingungen seines Dienstes einräumen zu lassen.[1240]

(5) Keine Aufsicht über den Nutzer gemäß § 10 S. 2 TMG

Der Anspruch auf die Haftungsbeschränkung entfällt weiterhin, wenn der Nutzer, der die Rechtsverletzung innerhalb des Internetdienstes des ISPs begeht, dem ISP untersteht oder von diesem beaufsichtigt wird. Ein Web 2.0-Dienst kann sich auf den Schutz der Haftungsbeschränkung somit nicht berufen, wenn der ISP den Nutzer in Bezug auf die Speicherung von Informationen in seinem Dienst anweisen und daher Art und Inhalt der gespeicherten Informationen effektiv kontrollieren

1235 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11 Rn. 50.
1236 *Freytag*, CR 2000, 600, 609; *Freytag,* in: *Lehmann* (Hrsg.), Electronic Business, 2002, Kap. F, Rn. 30.
1237 *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005 Teil D Rn. 64; *Spindler*, MMR-Beilage 7/200, 4, 18.
1238 BT-Drs. 14/6098, S. 25; *Sieber*/*Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 82; *Tettenborn/Bender/Lübben/Karenfort*, BB-Beilage 10/2001, 1, 33.
1239 *Sieber*/*Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 82; *Sobola/Kohl*, CR 2005, 443, 448; *Tettenborn/Bender/Lübben/Karenfort*, BB-Beilage 10/2001, 1, 33.
1240 *Spindler,* in: *Spindler/Schmitz/Geis, TDG, 2004* § 11 TDG Rn. 52; *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005 Teil D, Rn. 64; *Sobola/Kohl*, CR 2005, 443, 448.

kann.[1241] In dieser Einschränkung kommt die sowohl Art. 14 ECRL als auch § 10 TMG zugrunde liegende Annahme zum Tragen, dass ISPs vor allem deswegen schutzbedürftig sind, da sie den innerhalb ihrer Internetdienste stattfindenden Datenverkehr nicht kontrollieren können. Wie gezeigt wurde,[1242] bildet diese Annahme bildet eine der maßgeblichen Grundlagen für die Gewährung des besonderen Schutzes der Art. 12-14 ECRL bzw. §§ 8-10 TMG zugunsten von ISPs. Daraus folgt jedoch, dass seitens des ISPs der Anspruch auf die Haftungsbeschränkung entfallen muss, wenn der ISP den die jeweilige Informationen speichernden Nutzer und damit auch die gespeicherte Information kontrollieren kann, die Informationen somit seiner Sphäre zuzuordnen sind.[1243]

ff. Zwischenergebnis: Anwendbarkeit von § 10 TMG auf Web 2.0-Dienste in Bezug auf Schadensersatzansprüche

Der persönliche und sachliche Schutzbereich von § 10 TMG ist in Bezug auf die Tätigkeiten von ISPs, die Web 2.0-Dienste betreiben, regelmäßig eröffnet. Voraussetzung für die Anwendbarkeit der Haftungsbeschränkung ist weiterhin, dass ein ISP keine positive Kenntnis oder grob fahrlässige Unkenntnis von Urheberrechtsverletzungen hat. Die Analyse dieser subjektiven Voraussetzungen hat gezeigt, dass sich der (Nicht-)Einsatz von Content-Identification-Technologien insoweit weder positiv noch negativ auf einen ISP auswirkt. Soweit ein ISP somit nicht aufgrund anderer Umstände positive Kenntnis oder grob fahrlässige Unkenntnis von Urheberrechtsverletzungen hat, ändert auch der Einsatz von Content-Identification-Technologien bzw. der bewusste Verzicht hierauf nichts an diesem Ergebnis, d.h. wird die Anwendbarkeit der Haftungsbeschränkung hierdurch nicht erst ermöglicht oder aber ausgeschlossen. Sofern ein ISP zudem Urheberrechtsverletzungen nach Bekanntwerden unverzüglich aus seinem Internetdienst beseitigt und weiterhin die Nutzer, die innerhalb seines Internetdienstes Urheberrechtsverletzungen begehen, nicht seiner Aufsicht unterstehen, ist die Haftungsbeschränkung gemäß § 10 TMG auf ihn anwendbar.

1241 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11 Rn. 39.
1242 Vgl. 8. Kapitel, Teil C.I.1.d.aa.(2).
1243 *Tettenborn/Bender/Lübben/Karenfort*, BB-Beilage 10/2001, 1, 33; *Sobola/Kohl*, CR 2005, 443, 448.

e. Ergebnis

Gegen einen ISP, der einen Web 2.0-Dienst betreibt, in dessen Rahmen die Nutzer Urheberrechtsverletzungen begehen, kommt zwar grundsätzlich ein Schadensersatzersatzanspruch gemäß § 97 Abs. 2 S. 1 UrhG wegen eines Eingriffs in das Recht auf öffentliche Zugänglichmachung gemäß § 19 a UrhG in Betracht. Allerdings greift in Bezug auf die Dienstleistungen, die ein ISP im Rahmen von Web 2.0-Diensten erbringt, die Haftungsbeschränkung gemäß § 10 TMG ein.

Hierfür spielt keine Rolle, ob der ISP eine Content-Identification-Technologie einsetzt oder nicht. Denn im Rahmen von § 10 TMG führt nur positive Kenntnis bzw. im Zusammenhang mit Schadensersatzansprüchen grob fahrlässige Unkenntnis von der Rechtswidrigkeit einer Rechtsverletzung zum Ausschluss der Haftungsbeschränkung. Auf diese subjektiven Voraussetzungen wirkt sich jedoch weder der Einsatz einer Content-Identification-Technologie noch der bewusste Verzicht hierauf aus. In Bezug auf das Kriterium der grob fahrlässigen Unkenntnis, das im Falle eines urheberrechtlichen Schadensersatzanpruches die entscheidende Rolle spielt, folgt dieses Ergebnis daraus, dass gemäß § 7 Abs. 2 S. 1 TMG proaktive Überwachungspflichten eines ISPs grundsätzlich ausgeschlossen sind. Daher darf der Verzicht des ISPs auf die Ergreifung solcher Maßnahmen nicht zu Lasten des ISPs gehen. Dies wäre jedoch der Fall, wenn man aus dem Verzicht auf den Einsatz von Content-Identification-Technologien auf ein willentliches Sichverschließen vor der Kenntnis von Rechtsverletzungen und damit auf eine grob fahrlässig verursachte Unkenntnis des ISPs schließen würde.

Da somit alle Voraussetzungen von § 10 TMG erfüllt sind und diese Haftungsbeschränkung auf Web 2.0-Dienste anwendbar ist, scheidet eine Haftung dieser Dienste aufgrund der Wirkung der Haftungsbeschränkung als tatbestandsintegrierter Vorfilter bereits auf Tatbestandsebene aus.

2. Störerhaftung gemäß § 97 Abs. 1 S. 1 UrhG

Weiterhin kommen wegen der Urheberrechtsverletzungen, die die Nutzer im Rahmen von Web 2.0-Diensten begehen, negatorische Ansprüche gemäß § 97 Abs. 1 S. 1 UrhG gegen die Betreiber dieser Dienste in Betracht. Sind die Voraussetzungen der Störerhaftung erfüllt, besteht gegen den jeweiligen ISP ein Anspruch auf Unterlassung und/oder Beseitigung von Rechtsverletzungen.

a. Tatbestandsvoraussetzungen

Voraussetzung für einen Unterlassungs- oder Beseitigungsanspruch ist zunächst das Vorliegen der Störereigenschaft seitens des ISPs. Störer ist unabhängig von Art und Umfang des Tatbeitrags grundsätzlich jeder, der in irgendeiner Weise willentlich und adäquat kausal zur Verletzung eines geschützten Rechtsguts beiträgt.[1244] Hierfür kann genügen, dass die Handlung eines eigenverantwortlich handelnden Dritten unterstützt oder ausgenutzt wird, sofern der Inanspruchgenommene über die rechtliche Möglichkeit verfügt, die Verletzung des Rechtsguts zu verhindern.[1245] An die Störereigenschaft werden darüber hinaus keine weiteren Anforderungen gestellt, wie beispielsweise eine bestimmte Art von Tatbeitrag oder besondere subjektive Voraussetzungen.[1246] Daher kann auch derjenige, dessen eigenes Verhalten ihn weder als Täter noch als Mittäter, Anstifter oder Gehilfe einer fremden Urheberrechtsverletzung qualifiziert, dennoch als Störer auf Unterlassung und Beseitigung in Anspruch genommen werden.[1247]

Um jedoch eine unverhältnismäßige Ausuferung der Störerhaftung zu verhindern, wird im Falle von mittelbaren Rechtsgutsverletzungen im Bereich der wettbewerbsrechtlichen und urheberrechtlichen Störerhaftung die Haftung auf zumutbare Prüfungs- und Kontrollpflichten begrenzt.[1248] Die Beurteilung, ob eine Verletzung einer solchen Prüfpflicht vorliegt, richtet sich nach den jeweiligen Umständen des Einzelfalls unter Berücksichtigung der Funktion und Aufgabenstellung des als Störer Inanspruchgenommenen sowie der Eigenverantwortung des unmittelbar Handelnden.[1249] Weiterhin muss sich in der geltend gemachten Rechtsverletzung gerade die durch die Prüfpflichtverletzung herbeigeführte Gefährdungslage verwirklicht haben.[1250] Die Prüfpflicht besteht ab dem Zeitpunkt, in dem der

1244 *Wild*, in: *Schricker* (Hrsg.), UrhR, 2006, § 97, Rn. 36 a.; *Vinck*, in: *Loewenhein* (Hrsg.), HdB UrhR, 2010, § 81, Rn. 15; *J.B. Nordemann*, in: Fromm/Nordemann (Hrsg.), UrhR, 2008, § 97 UrhG, Rn. 156.

1245 St. Rspr., vgl. nur BGH vom 11.03.2004, GRUR 2004, 860, 864 – *Internet-Versteigerung I*; BGH vom 19.04.2007, GRUR 2007, 708 – *Internetversteigerung II*; BGH vom 15.10.1998, GRUR 1999, 418, 419 – *Möbelklassiker*; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 97, Rn. 33; *Nordemann,* in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 97 UrhG, Rn. 156; *Wild*, in: *Schricker* (Hrsg.), UrhR, 2006, § 97, Rn. 36 a; *Vinck*, in: *Loewenhein* (Hrsg.), HdB UrhR, 2010, § 81, Rn. 15; *J.B. Nordemann*, in: Fromm/Nordemann (Hrsg.), UrhR, 2008, § 97 UrhG, Rn. 156; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, § 8 TDG, Rn. 13; *Spindler/Volkmann*, WRP 2003, 1, 2.

1246 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, § 8 TDG, Rn. 13.

1247 *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 97, Rn. 33; *J.B. Nordemann*, in: Fromm/Nordemann (Hrsg.), UrhR, 2008, § 97 UrhG, Rn. 154.

1248 *Wild*, in: *Schricker* (Hrsg.), UrhR, 2006; § 97, Rn. 36 a; *J.B. Nordemann*, in: Fromm/Nordemann (Hrsg.), UrhR, 2008, § 97 UrhG, Rn. 157; *Vinck*, in: *Loewenhein* (Hrsg.), HdB UrhR, 2010, § 81, Rn. 15.

1249 BGH vom 11.03.2004, GRUR 2004, 860 – *Internet-Versteigerung I.*

1250 *Neubauer*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005, Teil D, Rn. 53 c; *Buschle*, in: *Moritz/Dreier*, RHdB E-Commerce, 2005, Teil D, Rn. 269;.

Störer auf die Rechtsverletzung hingewiesen wird, d.h. Kenntnis von der Rechtsverletzung erlangt.[1251]

Die Prüfpflicht muss dem Störer vor allem auch zumutbar sein.[1252] Neben der Erkennbarkeit des Rechtsverstoßes erfordert dies eine umfassende Abwägung der Interessen des Verletzten, des Störers und der Allgemeinheit,[1253] wobei insbesondere die Funktion und Aufgabenstellung des Störers sowie die Eigenverantwortung des unmittelbaren Rechtsverletzers von Relevanz sind.[1254] Darüber hinaus sind ähnliche Kriterien wie im Rahmen der Prüfung von Verkehrssicherungspflichten zu berücksichtigen.[1255] Es erfolgt somit eine Einzelfallbetrachtung, bei der die vom Störer geschaffenen Risiken sowie bestehende Kontroll- und Einflussmöglichkeiten für die Beurteilung der Haftung maßgeblich sind.[1256] Nur wenn diese Betrachtung ergibt, dass der vermeintliche Störer alles ihm Zumutbare getan hat, um den Eintritt der Rechtsverletzung zu verhindern, scheidet eine negatorische Haftung in seinem Fall aus.[1257] Sofern die Störerhaftung auf eine Prüfpflichtverletzung gestützt wird, richtet sich auch der Umfang der hieraus resultierenden Ansprüche nach dem Umfang der dem ISP zumutbaren Prüfpflichten.[1258]

Für einen Anspruch auf Unterlassung muss weiterhin Wiederholungsgefahr gegeben sein. Diese ist im Falle eines wiederherstellenden Unterlassungsanspruches, bei dem die Rechtsverletzung bereits begangen wurde, regelmäßig indiziert.[1259] Die Wiederholungsgefahr beschränkt sich nicht auf identische Rechtsverletzungen, sondern umfasst alle im Kern gleichartigen Verletzungsformen.[1260] Bei Geltendmachung eines vorbeugenden Unterlassungsanspruchs, der auf die Unterlassung einer noch nicht eingetretenen, zukünftig zu erwartenden Rechtsverletzung gerichtet ist, ist das Bestehen einer drohenden, hinreichend konkretisierten Erstbe-

1251 BGH vom 11.03.2004, GRUR 2004, 860, 864 – *Internet-Versteigerung I* ; BGH vom 19.04.2007, GRUR 2007, 708, 712 – *Internet-Versteigerung II*; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 97, Rn. 33; *J.B. Nordemann*, in: Fromm/Nordemann (Hrsg.), UrhR, 2008, § 97 UrhG, Rn. 158.

1252 BGH vom 11.03.2004, GRUR 2004, 860, 864 – *Internetversteigerung I;* BGH vom 19.04.2007, GRUR 2007, 708 – *Internetversteigerung II*; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 97, Rn. 33; *J.B. Nordemann*, in: Fromm/Nordemann (Hrsg.), UrhR, 2008, § 97 UrhG, Rn. 158; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 8, Rn. 22.

1253 *Freytag,* in: *Moritz/Dreier, RHdB E-Commerce, 2005,* Teil D, Rn. 114; *J.B. Nordemann*, in: Fromm/Nordemann (Hrsg.), UrhR, 2008, § 97 UrhG, Rn. 158; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 8, Rn. 23.

1254 BGH vom 01.04.2004, GRUR 2004, 693, 695 – *Schöner Wetten*.

1255 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 8, Rn. 23.

1256 *Klatt*, ZUM 2009, 265, 271.

1257 *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 97, Rn. 33.

1258 *Nordemann*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008, § 97 UrhG, Rn. 159; *Klatt*, ZUM 2009, 265, 266.

1259 St. Rspr, vgl. beispielsweise BGHZ 14, 163, 167 – *Constanze II*; *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 97, Rn. 41; *Wild*, in: *Schricker* (Hrsg.), UrhR, 2006, § 97, Rn. 42.

1260 BGH GRUR 1996, 290, 291, - *Wiederholungsgefahr I*; *Wild*, in: *Schricker* (Hrsg.), UrhR, 2006; § 97, Rn. 42.

gehungsgefahr erforderlich.[1261] Ein Anspruch auf Beseitigung des rechtswidrigen Zustands ist gegeben, wenn der das geschützte Rechtsgut gefährdende Störungszustand allein durch das Unterlassen der rechtsverletzenden Handlung nicht ausgeräumt wird.[1262] Ein durch einen rechtswidrigen Eingriff in ein Rechtsgut geschaffener fortdauernder störender Zustand muss somit durch den Störer beseitigt werden.[1263] Die Beseitigungsverpflichtung muss weiterhin verhältnismäßig, d.h. notwendig, geeignet und dem Störer zumutbar sein.[1264]

b. Anwendbarkeit von § 10 TMG auf Ansprüche der Störerhaftung

Wie dargelegt wurde, beschränkt § 10 TMG aufgrund der horizontalen Wirkung der Haftungsbeschränkungen die Haftung von ISPs in Bezug auf sämtliche Ansprüche, unabhängig davon, welchem Rechtsgebiet sie entstammen oder ob sie ein Verschulden erfordern. [1265] Demnach könnte § 10 TMG grundsätzlich auch auf Ansprüche der Störerhaftung Anwendung finden. Allerdings bleiben gemäß § 7 Abs. 2 S. 2 TMG „Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen … auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt". Mit dieser Regelung wurden Art. 12 Abs. 3, 13 Abs. 2 und 14 Abs. 3 ECRL[1266] in deutsches Recht umgesetzt, wonach die Haftungsbeschränkungen grundsätzlich „die Möglichkeit unberührt" lassen, dass „ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern". Diese Öffnungsklauseln wurden in § 7 Abs. 2 S. 2 TMG in einer einzigen Regelung zusammengezogen.[1267] Höchst umstritten ist in diesem Zusammenhang, was dies für das Verhältnis der Störerhaftung zu der Haftungsbeschränkung für Host-Provider gemäß § 10 TMG bedeutet.[1268]

1261 BGH vom 17.07.2003, GRUR 2003, 958 – *Paperboy*; *Freytag*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005, Teil D, Rn. 160; *Wild*, in: *Schricker* (Hrsg.), UrhR, 2006, § 97, Rn. 42.

1262 *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 97, Rn. 47; *Buschle*, in: *Moritz/Dreier*, RHdB E-Commerce, 2005, Teil D, Rn. 263.

1263 *Wild*, in: *Schricker* (Hrsg.), UrhR, 2006; § 97, Rn. 45.

1264 *Dreier*, in: *Dreier/Schulze*, UrhG, 2008, § 97, Rn. 48; *Wild*, in: *Schricker* (Hrsg.), UrhR, 2006, § 97, Rn. 47.

1265 Vgl. 8. Kapitel, Teil C.I.1.b.cc.

1266 Übereinstimmend heißt es insoweit in Art. 12 Abs. 3, 13 Abs. 2 und 14 Abs. 3 ECRL: *„Dieser Artikel läßt die Möglichkeit unberührt, daß ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern."*.

1267 BT-Drs. 14/6098, S. 23; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, § 8 TDG Rn. 3.

1268 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, § 8 TDG Rn. 15 ff.; *Sieber*/*Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 49.

aa. Die Rechtsprechung des BGH zu Internetversteigerungen

Seit der Entscheidung des BGH „Internetversteigerung I“ aus dem Jahr 2004[1269] ist ständige Rechtsprechung des BGH, dass die Haftungsbeschränkung für Host-Provider gemäß § 10 TMG auf die Störerhaftung nicht anwendbar ist. Demnach ist ein ISP weiterhin vollumfänglich negatorischen Ansprüchen der Rechtsinhaber ausgesetzt.

(1) Internetversteigerung I: Verpflichtung zur Beseitigung bekannter und zur Verhinderung kerngleicher Rechtsverstöße

Streitgegenstand der Entscheidungen des BGH waren jeweils Klagen des Herstellers von Uhren der Marke „Rolex“ sowie des Inhabers der in Bezug auf diese Uhren bestehenden Markenrechte („Kläger“) gegen den Betreiber des populären Internetauktionshauses Ebay („Beklagter“). Der Beklagte führte auf seinem Internetdienst Fremdversteigerungen durch. Die Parteien stritten darüber, inwieweit der Beklagte dafür haftete, dass er Dritten im Rahmen dieser Versteigerungen die Möglichkeit eröffnete, Plagiate der Uhren der Kläger anzubieten, in den Verkehr zu bringen und zu bewerben und hierdurch die Markenrechte der Kläger zu verletzen. Insoweit hatte der Beklagte im Hinblick auf § 11 TDG 2002 (nunmehr § 10 TMG) argumentiert, dass er den Nutzern lediglich eine technische Plattform zur Nutzung zur Verfügung stellen und die Versteigerungsangebote grundsätzlich in einem rein automatisierten Vorgang, d.h. ohne Kenntnisnahme durch einen Mitarbeiter, auf die Plattform gelangen würden. Allerdings kam der BGH in Bezug auf § 11 TDG 2002 zu dem Ergebnis, dass dieser auf Ansprüche der Störerhaftung grundsätzlich nicht anwendbar ist:

> „Der markenrechtliche Unterlassungsanspruch wird nicht dadurch ausgeschlossen, dass die Beklagte als Veranstalterin einer Plattform für Fremdversteigerungen nach dem Teledienstegesetz nur eingeschränkt haftet. ... Wie sich aus dem Gesamtzusammenhang der gesetzlichen Regelung ergibt, findet die Haftungsprivilegierung des § 11 TDG ... keine Anwendung auf Unterlassungsansprüche.“[1270]

Folglich kam nach Auffassung des BGH eine Haftung des Beklagten als Störer in Betracht, sofern dieser die allgemeinen Voraussetzungen der Störerhaftung erfüllte, d.h. die Rechtsverletzung willentlich und adäquat kausal mitverursacht und

1269 BGH vom 11.03.2004, GRUR 2004, 860ff.; vgl. hierzu die Anmerkungen von *Lehment*, GRUR 2005, 210 ff., sowie *Leible/Sosnitza*, NJW 2007, 3324 ff.
1270 BGH vom 11.03.2004, GRUR 2004, 860, 862.

weiterhin eine ihm obliegende Prüfpflicht verletzt hatte.[1271] Mit dieser Rechtsprechung schloss sich der BGH der von großen Teilen der Literatur seit der Umsetzung der ECRL in das TDG 2002 vertretenen Rechtsauffassung an,[1272] obwohl die Instanzrechtsprechung bereits wiederholt von der Anwendbarkeit der Haftungsbeschränkungen auch auf Ansprüche der Störerhaftung ausgegangen war.[1273]

Seine Rechtsauffassung begründete der BGH mit den folgenden Argumenten:[1274]

- Aus dem im Gesetz verwendeten Begriff der „Verantwortlichkeit" gehe hervor, dass die Haftungsbeschränkung sich nur auf verschuldensabhängige Ansprüche gegen den ISP beziehen könne, d.h. auf die strafrechtliche Verantwortung und Schadensersatzansprüche.
- Zudem gehe aus § 8 Abs. 2 S. 2 TDG 2002 (§ 7 Abs. 2 S. 2 TMG) hervor, dass die Störerhaftung von dem Anwendungsbereich der Haftungsbeschränkung ausgenommen sei. Dies entspreche auch dem Willen des europäischen Richtliniengebers, der die Ansprüche der Störerhaftung gegen ISPs nicht habe regeln wollen.
- Auch sei allein dieses Ergebnis interessengerecht, da ansonsten im Ergebnis an den Unterlassungsanspruch gegen den ISP höhere Anforderungen gestellt würden als an den Schadensersatzanspruch, da dieser bereits im Falle grob fahrlässiger Unkenntnis des ISP von der Rechtswidrigkeit einer Information oder Handlung eingreifen würde.
- Weiterhin werde dieses Resultat durch die Gesetzesbegründung zu § 5 Abs. 4 TDG 2002 gestützt, da auch hieraus hervorgehe, dass die Störerhaftung von ISPs von den Haftungsbeschränkungen habe unberührt bleiben sollen.

Konkret bedeutet dies für einen ISP, dass dieser, sobald ihm eine konkrete Rechtsverletzung bekannt geworden ist, das konkrete rechtswidrige Angebot unverzüglich sperren muss. Dies ergibt sich bereits aus § 10 S. 1 Nr. 2 TMG. Darüber hinaus muss er nach dem BGH in seiner Eigenschaft als Störer jedoch auch Vorsorge dafür treffen, dass es möglichst nicht zu „weiteren derartigen" Rechtsverletzungen kommt.[1275]

1271 BGH vom 11.03.2004, GRUR 2004, 860, 864.
1272 Vgl. nur Spindler/Schmitz/Geis/*Spindler*, TDG, TDG § 8 Rn. 15 ff; *Rössl/Rössl*, CR 2005, 809, 810; *Freytag*, CR 2000, 600, 605; *Spindler*, MMR Beilage 7/2000, 4, 20; *ders.*, MMR 2001, 737, 743; *Spindler/Volkmann*, WRP 2003, 1, 3 f.; *Lehment*, WRP 2003, 1058, 1063 f; *ders.,* GRUR 2005, 210 f.; *Stadler*, Informationen im Internet, 2005, Rn. 65; *Dustmann*, Privilegierte Provider, 2001, S. 109.
1273 Vgl. LG Düsseldorf MMR 2003, 120; OLG Düsseldorf MMR 2004, 315; OLG Brandenburg MMR 2004, 330; LG Berlin vom 25.02.2003, MMR 2004, 195.
1274 BGH vom 11.03.2004, GRUR 2004, 863, 864.
1275 BGH vom 11.03.2004, GRUR 2004, 864.

(2) Internetversteigerung II: Erstreckung der Verpflichtung auf zukünftige Verstöße

In seiner Entscheidung *Internet-Versteigerung II* bekräftigte der BGH die in der Entscheidung *Internetversteigerung I* artikulierten Grundsätze und baute sie weiter aus.[1276] Demnach kann ein ISP als Störer auch vorbeugend auf Unterlassung in Anspruch genommen werden, d.h. bereits dann, wenn eine Rechtsverletzung zwar noch nicht eingetreten ist, ihr Eintritt aber in Zukunft nach den Umständen zu befürchten ist und der ISP als potenzieller Störer eine Erstbegehungsgefahr begründet.[1277] Diese weitere Ausdehnung der Störerhaftung eines ISPs stützte der BGH auf den allgemeinen Grundsatz, dass bei einer drohenden Gefährdung nicht erst abgewartet werden muss, bis der erste Eingriff in das betroffene Rechtsgut auch tatsächlich erfolgt.[1278]

bb. Stellungnahme

Die vom BGH vertretene Rechtsauffassung, wonach aus § 7 Abs. 2 S. 2 TMG folgt, dass Ansprüche der Störerhaftung von den Haftungsbeschränkung für ISPs generell nicht erfasst werden, ist aus mehreren Gründen abzulehnen.

(1) Wortlaut von § 7 Abs. 2 S. 2 TMG

Ihrem Wortlaut nach lässt die Vorschrift gemäß § 7 Abs. 2 S. 2 TMG nur die „Entfernung" oder „Sperrung" von Informationen im Rahmen der allgemeinen Gesetze zu. Unter „Entfernung" kann dem Wortsinn nach jedoch nur die Beseitigung einer bereits eingetretenen Rechtsverletzung verstanden werden und unter „Sperrung" die Verhinderung ihrer fortgesetzten Nutzung für die Zukunft.[1279] Daraus geht hervor, dass die Haftungsvorschriften der allgemeinen Gesetze nur insoweit zum Tragen kommen können, als sie einen ISP zu eben diesen Handlungen – Sperrung und Entfernung – verpflichten, nicht aber, soweit sie darüber hinausgehende Haftungsfolgen wie beispielsweise eine in die Zukunft gerichtete Unterlassungsverpflichtung erlauben. Somit ergibt bereits die rein grammatikalische Auslegung von § 7 Abs. 2 S. 2 TMG, dass hierdurch nicht die Störerhaftung in Gänze vom An-

1276 BGH vom 19.04.2007, GRUR 2007, 708 – *Internetversteigerung II*; vgl. dazu *Wimmers/Heymann*, MR-Int 2007, 222 ff.
1277 BGH vom 19.04.2007, GRUR 2007, 708, 711.
1278 BGH s.o.
1279 *Leible/Sosnitza*, NJW 2004, 3225, 3226.

wendungsbereich der Haftungsbeschränkung ausgenommen werden sollte.[1280] Vielmehr erlaubt § 7 Abs. 2 S. 2 TMG seiner Formulierung nach nur einen Rückgriff auf die Ansprüche der Störerhaftung, soweit sie eine Art „Dauerbeseitigungsanspruch" zugunsten des Anspruchstellers gewähren. Nur diesem Teilanspruch sind ISPs dem Wortlaut der Vorschrift nach weiterhin ausgesetzt.[1281] Auf die Störerhaftung gestützte Ansprüche gegen einen ISP, gerichtet auf die Verhinderung zukünftiger, noch nicht eingetretener Rechtsverletzungen, scheiden hingegen aufgrund des Wortlauts von § 7 Abs. 2 S. 2 TMG von vornherein aus.

(2) Wortlaut und Zielsetzung der europarechtlichen Vorgaben

Weiterhin sprechen Wortlaut und Zielsetzung der Vorgaben der ECRL gegen eine generelle Ausnahme der Störerhaftung von dem Anwendungsbereich der Haftungsbeschränkung. In diesem Zusammenhang ist vor allem die Öffnungsklausel gemäß Art. 14 Abs. 3 ECRL maßgeblich, da Art. 14 ECRL das europarechtliche Pendant zu der Regelung gemäß § 10 TMG darstellt.

(i) Wortlaut

Zieht man die deutsche, englische und französische Fassung von Art. 14 ECRL heran und vergleicht sie mit dem Wortlaut von § 7 Abs. 2 S. 2 TMG, zeigt sich ein wesentlicher Unterschied zwischen der europarechtlichen Vorgabe und der deutschen Umsetzungsnorm.[1282] Denn die gerichtliche oder behördliche Maßnahme, die Art. 14 Abs. 3 ECRL ausnahmsweise gegen ISPs zulässt, hat einen individualisierten, konkreten Bezugspunkt, nämlich „die Rechtsverletzung" bzw. „an infringement" oder „une violation". Hingegen lässt § 7 Abs. 2 S. 2 TMG seinem Wortlaut nach generell „Verpflichtungen zur Entfernung oder Sperrung der Nut-

1280 *Leible/Sosnitza* s.o.

1281 *Hoeren,* in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010*,* Teil 18.2, Rn. 104; *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, Teil 18.1, Rn. 60; *Sobola/Kohl*, CR 2005, 443, 449; *Berger/Janal*, CR 2004, 917, 920; *Rücker*, CR 2005, 347, 350; *Volkmann*, CR 2003, 440, 446.

1282 Die deutsche, englische und französische Fassung von Art. 14 Abs. 3 1. Halbsatz ECRL lauten: *„Dieser Artikel lässt die Möglichkeit unberührt, dass ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern"*; *„This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement"*; *„Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation."*

zung von *Informationen* nach den allgemeinen Gesetzen ... auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 9 bis 11“[1283] zu. Durch diese Formulierung erscheint der Anwendungsbereich von § 10 TMG gegenüber Art. 14 Abs. 3 ECRL wesentlich weiter, da sich demnach hoheitliche Maßnahmen anscheinend gleich gegen mehrere Informationen auf einmal richten können. Hingegen geht aus der für Art. 14 ECRL gewählten Formulierung eindeutig hervor, dass sich eine hoheitliche Maßnahme immer nur gegen eine einzelne, bestimmte Rechtsverletzung richten kann.[1284]

Der Wortlaut von Art. 14 Abs. 3 ECRL, der aufgrund der Vollharmonisierung für die Auslegung des TMG allein maßgeblich ist, spricht somit dafür, dass nur einzelfallbezogene hoheitliche Maßnahmen in Bezug auf konkrete Rechtsverletzungen zulässig sind. Hingegen werden hierdurch nicht allgemein gefasste Verpflichtungen eines ISPs zur Beseitigung oder Vermeidung weiterer als der streitgegenständlichen Rechtsverletzung erlaubt, wie etwa die vom BGH für zulässig erklärte Unterlassungsverpflichtung in Bezug auf kerngleiche und zukünftige Verstöße.[1285]

(ii) Zielsetzung: Freistellung der Regelung des Verfahrens zur Beseitigung von Rechtsverletzungen

Zudem bezweckte der europäische Richtliniengeber mit der Öffnungsklausel gemäß Art. 14 Abs. 3 ECRL lediglich, den Mitgliedstaaten die Regelung des *Ver-*

1283 Hervorhebung durch die Verfasserin.

1284 Eine ähnliche sprachliche Unstimmigkeit besteht im Ersten Bericht über die Anwendung der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 08.06.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, KOM(2003) 702 endg. Dort heißt es in der deutschen Fassung des Berichtes, dass die ECRL die Möglichkeiten nationaler Gerichte oder Verwaltungsbehörden unberührt lasse, von einem Provider die Unterlassung oder Verhinderung „weiterer Rechtsverletzungen“ zu verlangen. Hingegen sind die englische bzw. französische Fassung des Berichts wiederum eindeutig so formuliert, dass hoheitliche Maßnahmen nur in Bezug auf „eine Rechtsverletzung“ zulässig sind. Hier wird der Unterschied noch deutlicher als im Rahmen von Art. 14 Abs 3, da sich die deutsche Fassung ihrer Formulierung nach fast ausschließlich auf zusätzliche, andere Rechtsverletzungen als die ursprünglich im Streit stehende zu beziehen scheint, während es nach der englischen und französischen Fassung des Berichtes nur um die Anordnung der Beseitigung oder Verhinderung einer einzelnen, konkreten Rechtsverletzung gehen kann.

1285 Dieses Ergebnis wird wiederum durch einen Passus im soeben (siehe vorhergende Fußnote) zitierten Bericht der Kommission bestätigt, wonach nach Auffassung der Kommission „Anlass zur Sorge“ besteht, wenn „Verfügungen im Rahmen einer allgemeinen Politik zur Bekämpfung unerlaubter Inhalte in größerem Umfang und nicht bei spezifischen Verstößen ausgesprochen“ werden. Als ein Beispiel für einen solchen Fall benennt der Bericht ausgerechnet einen Fall aus Nordrhein-Westfalen, in dem ca. 90 Anbieter von Internetzugängen von den Landesbehörden angewiesen worden waren, den Zugang zu bestimmten Seiten zu sperren; vgl. KOM(2003) 702 endg., Fn. 65.

fahrens freizustellen, mit dessen Hilfe die Rechtsinhaber die Entfernung oder Verhinderung einer konkreten Rechtsverletzung gegen einen ISP durchsetzen können. Darüber hinaus beabsichtigte er nicht, materiell-rechtliche Unterlassungs- und Beseitigungsansprüche von der Haftungsbeschränkung vollumfänglich auszunehmen.[1286] Dies geht deutlich aus dem Umstand hervor, dass der Europäische Richtliniengeber den Mitgliedsstaaten in Art. 14 Abs. 3 Hs. 2 ECRL die Möglichkeit einräumte, als Alternative zu behördlichen und gerichtlichen Maßnahmen zur Beseitigung von Rechtsverletzungen ein spezielles Verfahren zu schaffen:

> „Dieser Artikel läßt die Möglichkeit unberührt, daß ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern**,** oder daß die Mitgliedstaaten Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs zu ihr festlegen."[1287]

Mit der Regelung in Art. 14 Abs. 3 ECRL wurde somit „nur" beabsichtigt, den Mitgliedsstaaten einen Handlungsspielraum zur Sicherstellung einer möglichst effizienten Beseitigung von Rechtsverletzungen zu eröffnen. Zu diesem Zweck sollten sowohl die ISPs als auch – beispielsweise im Rahmen eines dem Notice&Takedown-Verfahren ähnlichen Prozederes – die betroffenen Rechtsinhaber herangezogen werden können, unabhängig davon, wer für die jeweilige Rechtsverletzung materiell-rechtlich verantwortlich zeichnet. Hierdurch sollte die Möglichkeit gewahrt bleiben, im Wege einer hoheitlichen Anordnung einen rechtswidrigen Zustand zu beseitigen und dadurch den grundrechtlich verbrieften Anspruch des betroffenen Rechtsinhabers auf effektiven Rechtsschutz gegen eine Rechtsverletzung sicherzustellen.[1288]

(3) Verstoß gegen den Ausschluss allgemeiner Überwachungspflichten

Die Erstreckung der Unterlassungspflichten von ISPs über eine konkrete Rechtsverletzung hinaus auch auf kerngleiche Verstöße steht zudem im scharfen Widerspruch zum Ausschluss allgemeiner Überwachungspflichten gemäß § 7 Abs. 2 S. 1 TMG. Denn hierdurch werden ISPs gezwungen, eine Kontrollinfrastruktur zu

1286 *Hoeren,* in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010*,* 18.2 Rn. 102; *Rücker*, CR 2005, 347, 350; vgl. auch Erwägungsgrund 45 ECRL: *„Die in dieser Richtlinie festgelegten Beschränkungen der Verantwortlichkeit von Vermittlern lassen die Möglichkeit von Anordnungen unterschiedlicher Art unberührt. Diese können insbesondere in gerichtlichen oder behördlichen Anordnungen bestehen, die die Abstellung oder Verhinderung einer Rechtsverletzung verlangen, einschließlich der Entfernung rechtswidriger Informationen oder der Sperrung des Zugangs zu ihnen."*

1287 Hervorhebung durch die Verfasserin.

1288 *Klatt*, ZUM 2009, 265, 270.

errichten, mit deren Hilfe aus allen eingestellten Informationen nach bestimmten Kriterien solche herausgesucht werden, die möglicherweise eine „kerngleiche" Rechtsverletzung darstellen und daher zu prüfen und gegebenenfalls zu beseitigen sind.[1289] Dies führt jedoch entgegen § 7 Abs. 2 S. 1 TMG bzw. Art. 15 Abs. 1 ECRL im Ergebnis zu einer Pflicht der ISPs zur Überwachung sämtlicher innerhalb ihrer Dienste vorhandenen Informationen.[1290] Aus diesem Grund gehen in der Literatur selbst diejenigen, die die Unanwendbarkeit von § 10 TMG auf Unterlassungsansprüche befürworten, davon aus, dass § 7 Abs. 2 S. 2 TMG nur behördliche oder gerichtliche Anordnungen zulässt, die auf die Sperrung oder Entfernung bestimmter rechtswidriger Informationen gerichtet sind, nicht hingegen darüber hinausgehende allgemeine Verpflichtungen zur Verhinderung auch kerngleicher Verstöße.[1291]

(4) Bedeutung der Störerhaftung im Bereich des Immaterialgüterrechtschutzes

Gegen die generelle Unanwendbarkeit der Haftungsbeschränkungen auf die Störerhaftung spricht nicht zuletzt auch, dass diese Ansprüche im Bereich des Imma-

1289 *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 57.

1290 *Hoeren,* in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010*,* 18.2 Rn. 103; *Freytag,* in: *Lehmann* (Hrsg.), Electronic Business, 2002, Kap. F, Rn. 11; *Berger/Janal*, CR 2004, 917, 919; *Wimmers/Heymann*, MR-Int 2007, 222, 223; vgl. 8. Kapitel, Teil C.I.1.b.ee.(3)(iv).

1291 *Spindler*, GRUR 2011, 101, 106; *Sieber/Höfinger*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010, 18.1, Rn. 48; *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 8 Rn. 35; *Buschle*, in: *Moritz/Dreier*, RHdB E-Commerce, 2005, Teil D, Rn. 276; *Sessinghaus*, WRP 2005, 697, 702; *Rücker*, CR 2005, 347, 351; *Sobola/Kohl*, CR 2005, 443, 449; *Spindler*, JZ 2005, 37, 39; *Hoeren*, MMR 2004, 672; *Spindler*/*Volkmann*, WRP 2003, 1, 14; *Volkmann*, CR 2003, 440, 447; *Spindler*, NJW 2002, 921, 925; *Freytag*, CR 2000, 600, 605; a.A. *Klatt*, ZUM 2009, 265, 275; *Rössl/Rössl*, CR 2005, 809, 813ff.; *Lehment*, WRP 2003, 1058, 1064. Von Vertretern der Gegenauffassung wird argumentiert, dass der unbestimmte Rechtsbegriff der allgemeinen Überwachungspflichten ein Ausfluss des Gebots der Zumutbarkeit sei und daher die insoweit entwickelten Kriterien weiterhin zur Bestimmung der Kontrollpflichten von ISPs herangezogen werden könnten, vgl. beispielsweise *Rössl/Rössl*, CR 2005, 808, 814; *Lehment*, WRP 2003, 1058, 1064. Diese Argumentation übersieht jedoch, dass in der Kodifizierung des Ausschlusses allgemeiner Überwachungsverpflichtungen die Entscheidung des europäischen Richtliniengebers zum Ausdruck kommt, basierend auf der Annahme der Unmöglichkeit effektiver Kontrolle von Informationen in Internetdiensten, ISPs grundsätzlich vom Einsatz solcher als unzumutbare Belastung angesehener Überwachungsmaßnahmen zu befreien und damit den Katalog an zumutbaren Maßnahmen von vornherein zu begrenzen. In der unveränderten Anwendung der althergebrachten allgemeinen Zumutbarkeitskriterien, die dieser Beschränkung des Pflichtenkreises der ISPs nicht Rechnung tragen, setzt sich diese Auffassung somit unzulässig über die Entscheidung des europäischen Richtliniengebers hinweg, die kraft dessen Einschätzungsprärogative verbindlich ist, vgl. *Rücker*, CR 2005, 347, 349, 353.

terialgüterrechtschutzes eine herausragende Rolle spielen.[1292] Ihre praktische Bedeutung nimmt gerade in Bezug auf die Haftung von ISPs ständig weiter zu, da für Rechtsinhaber oftmals die Inanspruchnahme des ISPs am naheliegendsten ist, weil die Belangung des unmittelbaren Täters vor allem aufgrund der Anonymität des Internets schwierig und darüber hinaus der ISP in der Regel der wirtschaftlich potentere Anspruchsgegner ist.[1293] Demgegenüber spielen Schadensersatzansprüche im deutschen Rechtskreis für die Rechtsinhaber eine eher untergeordnete Rolle, da die Substantiierung des entstandenen Schadens zumeist schwierig ist und die in diesem Zusammenhang durch die Gerichte zugesprochenen Beträge regelmäßig eher gering ausfallen.[1294]

Auch wurde gezeigt, dass die Passivlegitimation von ISPs für Schadensersatzansprüche aufgrund von Rechtsverletzungen der Nutzer schwer zu begründen ist, und insoweit höchstens Ansprüche im Zusammenhang mit der Verletzung von § 19 a UrhG in Betracht kommen. Dies bedeutet, dass Schadensersatzansprüche bereits aus diesem Grund, d.h. ungeachtet der Haftungsbeschränkung gemäß § 10 TMG, schwer durchsetzbar erscheinen.[1295] Hingegen bedeuten Unterlassungsansprüche für ISPs auch eine erhebliche finanzielle Belastung, da sie im Falle der erfolgreichen Inanspruchnahme die insoweit angefallenen Kosten der Rechtsverfolgung erstatten müssen und aus der Zuwiderhandlung gegen die Unterlassungsverpflichtung Ordnungsgelder und Vertragsstrafen resultieren können.[1296] Die wirtschaftlichen Folgen von Ansprüchen aus der Störerhaftung stellen somit für ISPs einen wesentlichen Faktor dar, den sie im Rahmen ihrer Geschäftsmodelle einkalkulieren müssen.

(5) Weitere Argumente des BGH

Auch die weiteren Argumente des BGH vermögen nicht zu überzeugen. Insbesondere kann die Rechtsauffassung, dass § 10 TMG nur auf verschuldensabhängige Ansprüche gegen den ISP Anwendung findet, nicht auf den Begriff der „Verantwortlichkeit“ gestützt werden. Denn wie bereits dargelegt wurde, kommt darin der rechtsgebietsübergreifende Charakter der Haftungsbeschränkungen zum Ausdruck

1292 *Freytag,* in: *Moritz/Dreier* (Hrsg.)*,* RHdB E-Commerce, 2005, Teil D, Rn. 111; *Heckmann,* in: *Heckmann*, jurisPK-Internetrecht, 2007, Vorbem. Kap. 1.7 Rn. 67; *Sobola/Kohl*, CR 2005, 443, 448; *Spindler*, MMR 2001, 737, 741.

1293 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, § 8 TDG Rn. 13; Sieber, CR 1997, 581; *Berger/Janal*, CR 2004, 917, 918.

1294 *Nordemann*, CR 2010, 653, 654; *Rücker*, CR 2005, 347, Fn. 4; *Berger/Janal*, CR 2004, 917, 919.

1295 Vgl. 8. Kapitel, Teil C.I.1.a.cc.

1296 *Volkmann*, Der Störer im Internet, 2005, S. 100; *Spindler*/*Volkmann*, WRP 2003, 1; *Hoeren*, MMR 2004, 672, 673; *Berger/Janal*, CR 2004, 917, 919.

und nicht eine Einschränkung von deren Anwendungsbereich auf bestimmte, verschuldensabhängige Haftungsnormen.

Auch kann der Argumentation nicht gefolgt werden, dass im Falle der Anwendbarkeit von § 10 TMG auch auf Ansprüche der Störerhaftung eine interessenwidrige Situation entstehen würde, indem dadurch im Ergebnis an die Haftung für Schadensersatzansprüche höhere Anforderungen zu stellen wären als an die negatorische Haftung. Insoweit ist ein Wechsel der Perspektive erforderlich, aus der die Betrachtung der Wirkung der Haftungsbeschränkungen erfolgt. Es ist zu vergegenwärtigen, dass durch § 10 TMG eine möglicherweise bestehende Haftung des ISPs zu dessen Gunsten eingeschränkt wird. Dies bedeutet jedoch umgekehrt, dass dem Rechtsinhaber durch die Haftungsbeschränkung Ansprüche genommen werden, die er ohne deren Eingreifen gegen den ISP geltend machen könnte. Vor diesem Hintergrund erscheint es durchaus gerechtfertigt, dass ein ISP höhere Anforderungen erfüllen muss, d.h. auch keine grob fahrlässige Unkenntnis von der Rechtswidrigkeit bestimmter Informationen oder Handlungen haben darf, um in den Genuss der Befreiung auch von immerhin verschuldensabhängigen Schadensersatzansprüchen zu kommen. Andererseits entsteht keine Schieflage dadurch, dass der ISP von negatorischen Ansprüchen, die gegenüber Schadensersatzansprüchen aufgrund der Nichterforderlichkeit eines Verschuldens den geringeren Unwertgehalt widerspiegeln, darüber hinaus solange befreit ist, bis ihm positive Kenntnis von der Rechtswidrigkeit einer Information oder Handlung nachgewiesen werden kann.

Zuletzt ist in diesem Zusammenhang anzumerken, dass die Gesetzesbegründung zum TDG 1997 aufgrund des Erlasses der ECRL sowie deren Umsetzung im TDG 2002 insbesondere in Bezug auf den vollharmonisierten Rechtsbereich der Providerhaftung nicht länger maßgeblich sein kann. Dass der BGH dennoch diese Gesetzesbegründung im Rahmen seiner Entscheidung herangezogen hat, trägt somit in keiner Weise dazu bei, den Überzeugungswert seiner Argumentation zu erhöhen.

cc. Ergebnis der BGH-Rechtsprechung: Rechtsunsicherheit über die Voraussetzungen der Haftung von Host-Providern

Dem europäischen Richtliniengeber ging es bei der Schaffung der Haftungsbeschränkungen jedoch gerade darum, wesentliche Haftungsrisiken für ISPs im Zusammenhang mit den von ihnen erbrachten Dienstleistungen zu minimieren oder zumindest kalkulierbar zu machen. Dieses Ziel würde jedoch weitgehend verfehlt, wenn die Störerhaftung vollumfänglich von den Haftungsbeschränkungen ausgenommen und damit die Haftung von ISPs weiterhin von der stark einzelfallabhängigen Auslegung der Voraussetzungen dieses Haftungsinstituts abhängig wä-

re.[1297] Dies zeigt sich bereits anschaulich an den Entscheidungen des BGH zu Internetversteigerungen, die zahlreiche, inhaltlich teilweise stark divergierende instanzgerichtliche Entscheidungen nach sich gezogen haben,[1298] woraus hervorgeht, dass unter den Gerichten mangels eines klaren Haftungsmaßstabs weitgehende Rechtsunsicherheit über die Voraussetzungen und den Umfang der Störerhaftung von ISPs für Rechtsverletzungen der Nutzer ihrer Internetdienste vorherrscht.[1299]

So bejahte das LG Hamburg die Störereigenschaft des beklagten ISP im Wesentlichen bereits aus dem Grund, dass Rechtsverletzungen über das Internet „allgemein zugenommen" hätten durch das Herunterladen und öffentliche Zugänglichmachen insbesondere auch urheberrechtlich geschützter Inhalte über das Internet.[1300] Daher berge der Internetdienst des Beklagten die „keinesfalls unwahrscheinliche Möglichkeit", dass von Dritten auch dort entsprechende Urheberrechtsverletzungen begangen würden. Da der ISP zudem „rechtlich und tatsächlich ... in die Lage versetzt gewesen" sei, wirksame Maßnahmen zur Verhinderung von Urheberrechtsverletzungen zu treffen, auf die im Urteil jedoch nicht weiter eingegangen wird, sah das Gericht die Störerhaftung als gegeben an.

Darüber hinaus fand das LG Düsseldorf, dass einem ISP, der weiß, dass mittels seines Internetdienstes Urheberrechtsverletzungen begangen werden, von denen er in nicht unerheblichem Maße profitiert, „besonders hohe Prüfungspflichten" obliegen.[1301] Der Umfang dieser Prüfpflichten könne so weit gehen, dass der ISP verpflichtet sei, auch Maßnahmen zu ergreifen, die sein Geschäftsmodell in wirtschaftlicher Hinsicht in Gänze in Frage stellten. Denn ebenso wie nicht jede Rechtsgutsverletzung einen „immensen Kontrollaufwand" rechtfertige, könne sich ein ISP nicht generell darauf berufen, dass eine effektive Kontrolle angesichts des massenhaften Datenverkehrs einen erheblichen und damit unzumutbaren Aufwand darstelle. Auch sei die Verhinderung von Urheberrechtsverletzungen ungeachtet der insoweit bestehenden technischen Möglichkeiten deswegen möglich, da der ISP „als letztes Mittel" jederzeit seinen Internetdienst einstellen könne. Eine Ab-

1297 *Sobola/Kohl*, CR 2005, 443, 449.

1298 OLG Düsseldorf vom 27.04.2010, ZUM 2010, 600; OLG Hamburg vom 30.09.2009, ZUM 2010, 440; OLG Düsseldorf vom 24.02.2009, MMR 2009, 402; LG Hamburg vom 12.06.2009, ZUM 2009, 863; LG Düsseldorf vom 23.01.2008, ZUM 2008, 338; OLG Saarbrücken vom 29.10.2007, MMR 2008, 343; LG Karlsruhe vom 10.12.2007, MMR 2008, 190; OLG Hamburg vom 26.09.2007, GRUR-RR 2008, 232; OLG Köln vom 21.09.2007, GRUR-RR 2008, 35; LG Hamburg vom 24.08.2007, MMR 2007, 726; LG München I vom 19.04.2007, MMR 2007, 453; OLG München vom 21.12.2006, GRUR-RR 2007, 393; OLG München vom 21.09.2006, MMR 2006, 739; LG Berlin vom 10.11.2005, ZUM 2006, 430.

1299 *Berger/Janal*, CR 2004, 917, 925.

1300 LG Hamburg vom 24.08.2007, MMR 2007, 726.

1301 LG Düsseldorf vom 23.01.2008, ZUM 2008, 338; ebenso LG Hamburg vom 12.06.2009, ZUM 2009, 863.

weichung von dem ansonsten gültigen Grundsatz, dass die eine Maßnahme zur Unterbindung von Rechtsverstößen nicht das gesamte Geschäftsmodell des potentiellen Störers in Frage stellen dürfe, sah das Gericht im konkreten Fall als gerechtfertigt an, da der Internetdienst der Beklagten offensichtlich auf die Begehung der urheberrechtsverletzenden Handlungen ausgerichtet sei.

Ebenso kam das OLG Hamburg zu dem Ergebnis, dass die zum Schutz gegen eine ausufernde Störerhaftung entwickelten Anforderungen an die Prüfpflichtverletzung auf den beklagten ISP nicht vollumfänglich Anwendung finden könnten, da dieser kein „von der Rechtsordnung gebilligtes Geschäftsmodell" betreibe, weil es auf die Förderung der massenhaften Begehung von Urheberrechtsverletzungen angelegt sei.[1302] Anderenfalls würden die Interessen der Schutzrechtsinhaber „institutionalisiert schutzlos" gestellt.

Zu einem ähnlichen Ergebnis kam auch das Hanseatische Oberlandesgericht, nämlich dass ein ISP sich nicht auf die faktische oder wirtschaftliche Unmöglichkeit der urheberrechtlichen Kontrolle seines Internetdienstes berufen kann, wenn der ISP Dritten unbegrenzte Möglichkeiten zur Begehung von Urheberrechtsverletzungen im eigenen wirtschaftlichen Interesse zur Verfügung stelle.[1303] Weiterhin ging das Gericht davon aus, dass die Begehung von Urheberrechtsverletzungen in Form des unerlaubten Hochladens urheberrechtlich geschützter Lichtbilder durch Einführung einer Pflicht zur namentlichen Registrierung der Nutzer effektiv verhindert werden könne. Bei der Registrierung sollten die Nutzer auch genaue Angaben zur in Bezug auf die Lichtbilder bestehenden Rechtekette machen. Auch sei die Beklagte aufgrund ihres Wissens, dass in der Vergangenheit bereits mehrfach Urheberrechtsverletzungen in ihrem Internetdienst begangen wurden, dazu verpflichtet, sämtliche Rechtsverletzungen dieser Art, „für die eine nicht unerhebliche Wahrscheinlichkeit" bestehe, zu unterbinden.

Andere Gerichte stellen hingegen wesentlich höhere Anforderungen an die Begründung der Haftung und den Umfang der Prüfungspflichten von ISPs. So sah das OLG Köln beispielsweise keine Anhaltspunkte dafür, dass der beklagten ISP von den Urheberrechtsverletzungen seiner Nutzer profitierte, da alle Nutzer für das Hochladen von Inhalten ein regelmäßiges monatliches Entgelt bezahlen mussten und das Herunterladen von Dateien kostenfrei war.[1304] Auch könne allein aus dem Umstand, dass der ISP den Vorgang des Herunterladens für solche Nutzer erleichtert habe, die sich kostenpflichtig registrieren lassen, nicht geschlossen werden, dass der ISP aus der Nutzung seines Internetdienstes durch Raubkopierer einen speziellen wirtschaftlichen Vorteil ziehen wolle.

1302 OLG Hamburg vom 30.09.2009, ZUM 2010, 440.
1303 OLG Hamburg vom 26.09.2007, GRUR-RR 2008, 230, 232 – *chefkoch.de*.
1304 OLG Köln vom 21.09.2007, GRUR-RR 2008, 35.

Auch wurde von Gerichten, die die Haftung von ISPs restriktiver bewerten, wiederholt betont, dass die einem ISP obliegenden Prüfungspflichten gerade nicht dazu führen dürften, das gesamte Geschäftsmodell des ISPs in Frage zu stellen.[1305] Daher werden Verpflichtungen zur manuellen Vor- oder auch Nachprüfung nach erfolgter Vorfilterung von auf einen Internetdienst durch Nutzer eingestellte Inhalte zumeist verneint, insbesondere wenn keine Technologien und/oder Merkmale ersichtlich sind, anhand derer rechtswidrige Inhalte effektiv ausgefiltert werden könnten.[1306] Allerdings geht aus den Entscheidungen hervor, dass der Einsatz einer solchen Filtertechnologie durchaus eine zumutbare Maßnahme im Rahmen der Prüfpflicht darstellt, sofern eine zusätzliche manuelle Nachprüfung gefundener „Treffer" überflüssig ist.[1307]

dd. Zusammenfassung: Anwendbarkeit von § 10 TMG auf Web 2.0-Dienste in Bezug auf negatorische Ansprüche

Die Auslegung von § 7 Abs. 2 S. 2 TMG unter Berücksichtigung der europarechtlichen Vorgaben der ECRL ergibt, dass Ansprüche der Störerhaftung nicht generell von dem Anwendungsbereich der Haftungsbeschränkungen ausgenommen sind, sondern nur behördliche oder gerichtliche Anordnungen gerichtet auf die Beseitigung oder Sperrung einzelner, konkretisierter Rechtsverletzungen.[1308] Durch § 7 Abs. 2 S. 2 TMG soll somit lediglich sichergestellt werden, dass die Beseitigung eingetretener Rechtsverletzungen trotz Einschlägigkeit der Haftungsbeschränkungen einer hoheitlichen Regulierung zugänglich bleibt.[1309] Die Verpflichtung des ISPs zur Beseitigung der Rechtsverletzung erfolgt insoweit unabhängig von der materiell-rechtlichen Haftung des ISPs und damit auch unabhängig vom Vorliegen

1305 LG Karlsruhe vom 10.12.2007, MMR 2008, 190; LG München I vom 19.04.2007, MMR 2007, 453; OLG München vom 21.12.2006, GRUR-RR 2007, 393 sowie vom 21.09.2006, MMR 2006, 739, das als eines der wenigen Gerichte auch darauf hinweist, dass eine allgemeine Verpflichtung zur inhaltlichen Prüfung aller Informationen und Inhalte eines Internetdienstes gegen das Verbot allgemeiner Überwachungspflichten gemäß § 7 Abs. 2 S. 1 TMG verstoßen würde.

1306 LG Karlsruhe vom 10.12.2007, MMR 2008, 190; OLG Köln vom 21.09.2007, GRUR-RR 2008, 35; LG München I vom 19.04.2007, MMR 2007, 453; OLG München vom 21.12.2006, GRUR-RR 2007, 393.

1307 LG München I vom 19.04.2007, MMR 2007, 453; OLG München vom 21.12.2006, GRUR-RR 2007, 393.

1308 So auch *Berger/Janal* s.o.; *Sobola/Kohl*, CR 2005, 443, 450; *Wimmers/Heymann*, MR-Int 2007, 222, 223.

1309 *Engels*, AfP 2000, 524, 529.

weiterer, insbesondere auch subjektiver[1310] Voraussetzungen. Vielmehr wird auf den ISP zum Zwecke der Beseitigung von rechtswidrigem Material allein aufgrund der Tatsache seiner technischen Nähe zu der Rechtsverletzung zugegriffen. Weitere Pflichten des ISPs ergeben sich hieraus jedoch nicht, insbesondere nicht die weiterreichenden Unterlassungsverpflichtungen der Störerhaftung, die sich auch auf die Beseitigung und Verhinderung kerngleicher sowie zukünftiger Rechtsverletzungen richten können. Will ein Urheber sich dennoch die Möglichkeit offenhalten, solche weitergehenden Rechtsansprüche gegen den ISP geltend machen zu können, muss er dem ISP eine Rechtsverletzung konkret anzeigen. Als Folge hieraus entfällt die Haftungsbeschränkung gemäß § 10 S. 1 Nr. 1 TMG wegen positiver Kenntnis des ISPs von der Rechtsverletzung, es sei denn, der ISP ergreift unverzüglich Maßnahmen zur Beseitigung des angezeigten rechtswidrigen Materials.

Der vom BGH vertretenen Auffassung, dass die Störerhaftung vom Anwendungsbereich der Haftungsbeschränkungen von vornherein ausgenommen ist, kann demgegenüber nicht gefolgt werden. Denn eine solche Auslegung von § 7 Abs. 2 S. 2 TMG steht im Widerspruch zu den europarechtlichen Vorgaben und würde die mit den Haftungsbeschränkungen hauptsächlich verfolgte Zielsetzung der Schaffung von Rechtssicherheit für ISPs weitgehend vereiteln.[1311]

Als Ergebnis bleibt somit festzuhalten, dass § 10 TMG auch auf Ansprüche der Störerhaftung anwendbar ist. Negatorische Ansprüche gegen einen ISP, der einen Web 2.0-Dienst betreibt, sind somit grundsätzlich ebenfalls ausgeschlossen. Auf-

1310 Nach dem BGH ist im Einklang mit den in Bezug auf die mittelbare Störerhaftung im Erfolgsunrecht entwickelten Grundsätzen Voraussetzung für die Prüfpflicht und damit für eine mögliche Unterlassungsverpflichtung des ISPs, dass dieser positive Kenntnis von der Rechtsverletzung hat, vgl. *Wiebe*, in: *Ernst/Vassilaki/Wiebe*, Hyperlinks, 2002, Rn. 144; *Freytag,* in: *Lehmann* (Hrsg.), Electronic Business, 2002, Kap. F, Rn. 40. Denn der Gesetzgeber habe bei Erlass des TDG 1997/TMG nicht beabsichtigt, an der bis dato unter § 5 Abs. 4 TDG 1997 geltenden Rechtslage etwas zu ändern, wonach die den Providern gemäß den Grundsätzen der Störerhaftung obliegenden Prüfpflicht nur die Prüfung der Rechtswidrigkeit bereits bekannter Inhalte erfasste, vgl. BT-Drs. 14/6098, S. 23. Zudem ergebe sich dieses Erfordernis mittelbar aus dem Ausschluss allgemeiner Überwachungspflichten gemäß § 7 Abs. 2 S. 1 TMG, da ansonsten die Provider zum Zwecke der Vermeidung der negativen Folgen einer Haftung dazu gezwungen wären, ihnen unbekannte Informationen zur Kenntnis zu nehmen und auf ihre Rechtmäßigkeit hin zu überprüfen, vgl. *Spindler*/*Volkmann*, WRP 2003, 1, 4. Darüber hinaus wird in Bezug auf das Kenntniserfordernis gefordert, dass auch bereits das Vorliegen von grob fahrlässiger Unkenntnis von Umständen, aufgrund derer eine Rechtsverletzung evident ist, zur Begründung eines negatorischen Anspruches gegen den ISP ausreichen müsse, um einen „Gleichlauf" zwischen der Störerhaftung und der Schadensersatzhaftung zu erreichen, d.h. zu vermeiden, dass der ISP im Falle grob fahrlässiger Unkenntnis von einer rechtswidrigen Information zwar auf Schadensersatz hafte, von ihm mangels positiver Kenntnis jedoch nicht die Sperrung oder Entfernung der Information verlangt werden könne, vgl. *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 8 Rn. 20; Sieber/Höfinger, in: Hoeren/Sieber (Hrsg.), Multimediarecht, 2010, Teil 18.1, Rn. 51; *Spindler*/*Volkmann*, WRP 2003, 1, 4.

1311 So auch *Rücker*, CR 2005, 347, 348; *Berger/Janal*, CR 2004, 917, 925; a.A. *Rössl/Rössl*, CR 2005, 809ff; *Sobola/Kohl*, CR 2005, 443, 450.

grund von § 7 Abs. 2 S. 2 TMG kann der ISP nur zu der Beseitigung konkreter, individualisierter und bereits eingetretener Rechtsverletzungen verpflichtet werden.[1312]

c. Auswirkungen von Content-Identification-Technologien auf die Störerhaftung von Web 2.0-Diensten

Die Auswirkungen von Content-Identification-Technologien auf die Störerhaftung von Web 2.0-Diensten werden nachfolgend zunächst auf der Grundlage der BGH-Rechtsprechung zu Internetversteigerungen dargestellt. Sodann werden ihre Auswirkungen unter der hier vertretenen Rechtsauffassung beschrieben, dass § 10 TMG grundsätzlich auch auf Ansprüche der Störerhaftung anwendbar ist.

aa. Auswirkungen unter Zugrundelegung der BGH-Rechtsprechung zu Internetversteigerungen

Wenn man wie der BGH davon ausgeht, dass § 10 TMG auf die Ansprüche der Störerhaftung grundsätzlich nicht anwendbar ist, haftet der ISP nach den allgemeinen Grundsätzen der Störerhaftung bei mittelbaren Rechtsverletzungen.[1313] Fraglich ist, wie sich die Verfügbarkeit von Content-Identification-Technologien auf das Vorliegen der insoweit für die Haftung des mittelbaren Rechtsverletzers maßgeblichen Prüfpflichtverletzung auswirkt.

(1) Erforderliche Maßnahmen seitens des ISP zur Erfüllung der Prüfpflicht

In Bezug auf die Zumutbarkeit einer Prüfpflicht betreffend die im Internetdienst des Beklagten vorhandenen Informationen stellte der BGH in der Entscheidung *Internetversteigerung I* klar, dass dem Beklagten grundsätzlich nicht zugemutet werden kann, jedes einzelne Angebot vor der Veröffentlichung auf seine Rechtswidrigkeit hin zu untersuchen. Denn eine solche Verpflichtung würde das gesamte

1312 Eine ansatzweise Klärung dieser Streitfrage durch den EuGH wird vom Ausgang des Vorabentscheidungsersuchens des High Court of Justice von England und Wales im Zusammenhang mit einem in England anhängigen Rechtstreit erwartet, vgl. die Schlussanträge des Generalanwalts Niilo Jääskinen im Verfahren „L'Oreal/eBay" vom 09.12.2010 – C-324/09.

1313 Vgl. 8. Kapitel, Teil C.I.2.b.aa.

Geschäftsmodell des Beklagten in Frage stellen.[1314] Jedoch ist zu berücksichtigen, dass der Beklagte auch von dem Verkauf von Plagiaten über seine Plattform durch die ihm insoweit zustehende Provision profitiert. Daher ist seinem Interesse an einem möglichst kostengünstigen Ablauf des Geschäftsbetriebes grundsätzlich ein geringeres Gewicht zuzumessen.

Hinsichtlich der konkret an den beklagten ISP zu stellenden Anforderungen zur Erfüllung der Unterlassungsverpflichtung bei Bekanntwerden von Urheberrechtsverletzungen hielt sich der BGH in seinen Entscheidungen bisher zurück. In der Entscheidung *Internetversteigerung I* beließ es der BGH insoweit anstatt einer konkreten Verpflichtung des ISPs zur Ergreifung bestimmter Maßnahmen – wie beispielsweise dem Einsatz einer „Filtersoftware", den der BGH dem beklagten ISP in der Entscheidung zwar grundsätzlich nahelegte, ihn aber nicht ausdrücklich darauf verpflichtete[1315] – sogar nur bei dem lapidaren Hinweis, dass auch ein als Störer verurteilter und einem Unterlassungstitel unterworfener ISP im Vollstreckungsverfahren gemäß § 890 ZPO nur für eine schuldhafte Zuwiderhandlung gegen die ihm auferlegte Unterlassungsverpflichtung haftbar gemacht werden kann. Spätestens hier muss somit berücksichtigt werden, ob der ISP eine Rechtsverletzung, beispielsweise durch ein vorgeschaltetes Filterverfahren, hätte aufdecken können.[1316] Damit verlagerte der BGH jedoch die Prüfung der Zumutbarkeit bestimmter Kontrollmaßnahmen im Ergebnis in das Vollstreckungsverfahren.[1317] Mittlerweile hat der BGH jedoch insoweit klargestellt, dass ein Gericht bereits bei der Prüfung der Begründetheit eines Unterlassungsanspruch grundsätzlich auch berücksichtigen muss, inwieweit es dem beklagten ISP im konkreten Fall tatsächlich technisch möglich und zumutbar ist, weitere Rechtsverletzungen zu verhindern.[1318]

In der Entscheidung *Internetversteigerung II* ging der BGH weiterhin ausdrücklich davon aus, dass zur praktischen Umsetzung der vorbeugenden Unterlassungsverpflichtung des Beklagten auch der Einsatz einer Filtersoftware „in gewissem Umfang" zur Aufdeckung von Verdachtsfällen geboten war. Die hierdurch generierten Treffer mussten darüber hinaus gegebenenfalls zusätzlich manuell nachgeprüft werden. Die Grenze des dem Beklagten insoweit Zumutbaren ist aber jedenfalls dann erreicht, wenn im konkreten Fall keine für das Suchsystem geeigneten

1314 BGH vom 11.03.2004, GRUR 2004, 860, 864 – *Internetversteigerung I*; ebenso LG Düsseldorf vom 29.10.2002, MMR 2003, 120; OLG Brandenburg vom 16.12.2003, MMR 2004, 330.

1315 BGH vom 11.03.2004, GRUR 2004, 860, 864 – *Internetversteigerung I*.

1316 BGH s.o.

1317 Krit. hierzu *Stadler*, Informationen im Internet, 2005, Rn. 69 a; *Volkmann*, Der Störer im Internet, 2005, S. 184 ff.

1318 BGH vom 10.04.2008, GRUR 2008, 1097, 1099; vgl. hierzu *Volkmann*, CR 2009, 361, 363.

Merkmale zur Aufdeckung von Verdachtsfällen vorliegen.[1319] Andererseits hindert die Tatsache, dass „eine lückenlose Vorabkontrolle, die sämtliche Rechtsverletzungen sicher erkennt, technisch nicht möglich" ist, grundsätzlich nicht die Verurteilung des betroffenen ISP zur Unterlassung.[1320]

Aus der Entscheidung *Internetversteigerung III* geht weiterhin hervor, dass eine schuldhafte Verletzung einer Unterlassungsverpflichtung dann ausscheidet, wenn die Rechtsverletzungen nicht durch den Einsatz eines zumutbaren Filterverfahren einschließlich manueller Nachprüfung der Ergebnisse hätten erkannt werden können.[1321] Diesen Grundsatz hat der BGH in einer späteren Entscheidung bekräftigt und präzisiert.[1322] Demnach dürfen dem ISP „keine Anforderungen auferlegt werden, die ihr von der Rechtsordnung gebilligtes Geschäftsmodel gefährden oder ihre Tätigkeit unverhältnismäßig erschweren".[1323] Eine Überprüfung der auf einer Internetplattform eingestellten Angebote ist daher nur zumutbar, sofern dem ISP eine Filtersoftware zur Verfügung steht, die Verdachtsfälle verlässlich aufspüren kann; nicht zumutbar ist dem ISP hingegen eine Kontrollverpflichtung, wenn die relevanten Rechtsverletzungen nicht durch eine Filtersoftware aufgespürt werden können und daher jedes einzelne verdächtige Angebot zusätzlich einer manuellen Kontrolle unterzogen werden muss.[1324]

Nach der Entscheidung *Kinderhochstühle im Internet* deutet sich an, dass eine Kontrollverpflichtung für den ISP nach Abwägung der wechselseitigen Interessen möglicherweise auch dann als unzumutbar anzusehen ist, wenn der von einer Rechtsverletzung betroffene Rechtsinhaber ebenso wie der ISP in der Lage ist, die Überprüfung der auf dem Internetdienst vorhandenen Angebote durchzuführen.[1325] In dem der Entscheidung zugrundeliegenden Fall hatte die beklagte Betreiberin einer Internetauktionsplattform den Inhabern von Schutzrechten die Möglichkeit eingeräumt, Schutzrechtsverletzungen mit Hilfe einer Suchfunktion („VeRI-Programm") aufzufinden. Mit diesem Programm konnten auf der Plattform eingestellte Angebote herausgefiltert werden, die bestimmte Markenbegriffe enthielten. Die Schutzrechtsinhaber konnten diese Angebote sodann auf ihre Rechtmäßigkeit hin überprüfen. Wurde ein rechtsverletzendes Angebot auf diese Weise identifiziert, gab die Beklagte die dieses Angebot betreffenden Nutzerdaten an den betroffenen Schutzrechtsinhaber heraus. Vor diesem Hintergrund vertrat der BGH die Auffassung, das es „nicht ohne Weiteres einzusehen" sei, „warum die Beklagte

1319 BGH vom 19.04.2007, GRUR 2007, 708, 712 – *Internetversteigerung II*.
1320 BGH s.o.
1321 BGH vom 30.04.2008, GRUR 2008, 702, 706 – *Internetversteigerung III*.
1322 BGH vom 22.07.2010, GRUR 2011, 152 – *Kinderhochstühle im Internet*; vgl. hierzu die Besprechung von *Spindler*, GRUR 2011, 101 ff.
1323 BGH vom 22.07.2010, GRUR 2011, 152, 155 – *Kinderhochstühle im Internet*.
1324 BGH s.o.
1325 BGH s.o.

[der ISP] der Klägerin [der Rechtsinaberin] eine Überprüfung … abnehmen soll, die die Klägerin als Schutzrechtsinhaberin mit gleichem Aufwand selbst bewerkstelligen kann."[1326] Im Ergebnis lehnte der BGH daher eine Prüfpflichtverletzung und damit die Störerhaftung des beklagten ISPs ab.

(2) Bewertung

Nach der Rechtsprechung des BGH zu Internetversteigerungen ist ein ISP zur Erfüllung der ihm obliegenden Prüfpflicht grundsätzlich auch zum Einsatz technischer Hilfsmittel verpflichtet, wie beispielsweise einer Filtersoftware, mithilfe derer vorhandene Informationen anhand bestimmter Kriterien gefiltert werden. Es kommt somit grundsätzlich auch eine Verpflichtung von ISPs zum Einsatz einer Content-Identification-Technologie zur Erfüllung der Prüfpflicht in Betracht. Maßgeblich ist insoweit allein, ob diese Technologien technisch dazu geeignet sind, Rechtsverletzungen zu verhindern und ihr Einsatz dem ISP nicht aus anderen Gründen unzumutbar ist.

Von der technischen Fähigkeit von Content-Identification-Technologien, Rechtsverletzungen zu beseitigen und zu verhindern, kann – wie in dieser Arbeit ausführlich dargestellt wurde – ausgegangen werden.[1327] Der Einsatz einer Content-Identification-Technologie ist daher grundsätzlich geeignet, Urheberrechtsverletzungen zu verhindern, vor allem auch deswegen, da solche Verletzungen bereits im Zuge des Hochladens einer Datei auf einen Web 2.0-Dienst erkannt werden können und insbesondere bestimmte Audio-Fingerprinting-Technologien eine hohe Treffsicherheit für sich beanspruchen können.[1328] In Bezug auf die Zumutbarkeit ist weiterhin zu prüfen, ob der Einsatz einer solchen Technologie einem durchschnittlichen ISP wirtschaftlich zumutbar ist. Insoweit ist jedoch zu berücksichtigen, dass der BGH klargestellt hat, dass die wirtschaftlichen Interessen des ISP im Rahmen der Bestimmung der Zumutbarkeit einer Maßnahme aufgrund des wirtschaftlichen Eigeninteresses des ISP an den Rechtsverletzungen nur eine untergeordnete Rolle spielen können. Ihm ist daher grundsätzlich zuzumuten, in gewissem Maße Kosten für die Gewährleistung des Schutzes der Rechte Dritter aufzuwenden.

1326 BGH s.o.

1327 Vgl. 7. Kapitel, Teil B.

1328 Zur Treffsicherheit beispielsweise der Audio-Fingerprinting-Technologie von Audible Magic vgl. 7. Kapitel, Teil B.II.1; zur Relevanz der Treffsicherheit von Filterprogrammen im Zusammenhang mit der Beurteilung der Zumutbarkeit vgl. z.B. LG Düsseldorf vom 29.10.2002, MMR 2003, 120. Das LG Düsseldorf hat weiterhin entschieden, dass die Filterung von Inhalten mit einem MD-5-Filter, d.h. einem einfachen Hash-Filter (vgl. hierzu vgl. 7. Kapitel, Teil B.I.) ungeeignet ist, um die einem ISP obliegende Prüfpflicht zu erfüllen, LG Düsseldorf vom 23.01.2008, ZUM 2008, 338; ebenso LG Hamburg vom 12.06.2009, ZUM 2009, 863.

Dementsprechend ist der Einsatz einer Content-Identification-Technologie aus Gründen der Wirtschaftlichkeit nur dann abzulehnen, wenn der ISP darlegen kann, dass die Implementierung solcher Technologien für ihn eine unzumutbare Härte darstellen würde, die sein gesamtes Geschäftsmodell in Frage stellt.

Die Prüfpflicht des Störers bezieht sich grundsätzlich (nur) auf Rechtsverletzungen, die dem ISP bekannt sind. Nach der Rechtsprechung des BGH zu Internetversteigerungen bezieht sie sich darüber hinaus auf Rechtsverletzungen, die mit denjenigen, die dem ISP bekannt sind, kerngleich sind. Auch werden zukünftige Rechtsverletzungen dieser Art von der Prüfpflicht des ISPs erfasst. Somit muss ein ISP die Content-Identification-Technologie nur zum Schutz solcher urheberrechtlich geschützte Multimediawerke einsetzen, bezüglich derer Rechtsverletzungen bereits bekannt sind. Fraglich ist jedoch, wie sich auf den Umfang dieser Verpflichtung auswirkt, dass der ISP nach der Rechtsprechung des BGH auch „kerngleiche" Rechtsverletzungen verhindern muß. Damit werden auch Verletzungen in Bezug auf „charakteristisch gleichartige Rechtsgüter" in die Unterlassungsverpflichtung des ISPs einbezogen.[1329] Bei entsprechend weiter Auslegung des Begriffs der Kerngleichheit könnte hierfür jedoch bereits ausreichen, dass aus den bekannten Rechtsverletzungen genug Merkmale hervorgehen, die einen Rückschluss auf weitere von Rechtsverletzungen betroffene Rechtsgüter zulassen.[1330]

Darüber hinaus lassen die Argumente und der generelle Ton der BGH-Rechtsprechung zu Internetversteigerungen darauf schließen, dass sich darin die grundsätzliche Auffassung das Gerichts niederschlägt, wonach Internetdienste aufgrund ihrer Missbrauchsanfälligkeit für Rechtsverletzungen tendenziell als eine Gefahrenquelle anzusehen sind.[1331] Es würde daher nicht überraschen, wenn der BGH ISPs absehbar entsprechend der zu Verkehrssicherungspflichten entwickelten Grundsätze[1332] dazu verpflichten würde, alle geeigneten und zumutbaren Gegenmaßnahmen zu ergreifen, um der Realisierung dieser Gefahren soweit wie möglich entgegenzuwirken.[1333] Hierunter fiele dann auch die Möglichkeit, Content-Identi-

1329 *Klatt*, ZUM 2009, 265, 273.
1330 *Klatt*, ZUM 2009, 265, 274.
1331 So auch *Spindler*, GRUR 2011, 101, 107.
1332 In der Literatur wird z.T. die Auffassung vertreten, dass für die Beurteilung der Haftung von ISPs anstatt der Prüfung einer Prüfpflichtverletzung im Sinne der sachenrechtlichen Störerhaftung generell der Rückgriff auf das deliktsrechtliche Institut der Verkehrssicherungspflichten erwogen werden sollte, vgl. dazu *Klatt*, ZUM 2009, 265 ff; der BGH lehnt jedoch bisher die Heranziehung der deliktsrechtlichen Kategorien der Täterschaft und Teilnahme zur Begründung der Passivlegitimation im Zusammenhang mit Unterlassungsansprüchen bei der Verletzung absoluter Rechtsgüter, und damit auch für die Verletzung von Urheberrechten, ab, vgl. BGH vom 30.06.2009, MMR 2009, 752 – *Störerhaftung des Verpächters einer Domain*.
1333 *Rössl/Rössl*, CR 2005, 809, 812; allerdings bezwecken die Haftungsbeschränkungen gerade klarzustellen, dass Internetdienste grundsätzlich als sozialadäquate, d.h. nicht besondere Gefahrquellen darstellende Dienstleistungen anzusehen sind, vgl. 8. Kapitel, Teil C.I. 1.b.dd.

fication-Technologien einzusetzen, und zwar nicht nur zur Verhinderung bereits bekannter und damit kerngleicher Rechtsverletzungen, sondern darüber hinaus zum Schutz sämtlicher urheberrechtlich geschützter Werke, deren rechtswidrige Nutzung im Rahmen des Internetdienstes des ISPs theoretisch in Betracht kommt.

Allerdings stünde einer solchen Ausdehnung der Verpflichtung der ISPs zur Verhinderung von Rechtsverletzungen im weitest möglichem Umfang an und für sich der Ausschluss allgemeiner Überwachungspflichten gemäß § 7 Abs. 2 S. 1 TMG entgegen. Denn aus der Kombination des Ausschlusses einer generellen Verpflichtung zur Überwachung der Tätigkeiten der Nutzer mit den subjektiven Voraussetzungen für den Verlust der Haftungsbeschränkung gemäß § 10 S. 1 Nr. 1 TMG ergibt sich eindeutig, dass ein ISP keinerlei besondere Maßnahmen ergreifen muss, um Rechtsverletzungen aufzudecken. Es besteht somit auch keine Verpflichtung zum Einsatz einer besonderen Software zur Verhinderung von Rechtsverletzungen.[1334] Dieser Einwand dürfte den BGH bei seiner Entscheidung über den Umfang der Pflicht zum Einsatz von Content-Identification-Technologien jedoch kaum beeinträchtigen, da er diesen Vorwurf, der von weiten Teilen der Literatur bereits in Bezug auf die durch ihn ausgesprochene Verpflichtung von ISPs Verpflichtung zur Verhinderung auch „kerngleicher" Verstöße erhoben wurde, in seinen weiteren Entscheidungen nicht berücksichtigt hat.

Einen Ausweg aus diesem Dilemma zeigt möglicherweise die Entscheidung *Kinderhochstühle im Internet*.[1335] Darin hat der BGH die Zumutbarkeit einer Prüfpflicht des ISPs verneint, wenn der Rechtsinhaber über dieselben technischen Möglichkeiten wie der ISP verfügt, um Rechtsverletzungen in dem Internetdienst aufzuspüren, da der ISP nicht ohne weiteres verpflichtet ist, dem Rechtsinhaber diese Arbeit abzunehmen. Dies bedeutet, dass es seitens des ISPs ausreichen kann, den Rechtsinhabern bestimmte technische Werkzeuge zur Identifikation von Rechtsverletzungen zur Verfügung zu stellen, um eine Störerhaftung abzuwenden. Auf diese Weise müsste der ISP die Filterung rechtswidriger Angebote nicht mehr selbst durchführen, sondern könnte dies den Rechtsinhabern überlassen und seinen eigenen Aufwand in dieser Hinsicht auf die Zurverfügungstellung der entsprechenden Technologien beschränken.

bb. Auswirkungen bei ECRL-konformer Auslegung von § 7 Abs. 2 S. 2 TMG

Die Analyse der Regelung gemäß § 7 Abs. 2 S. 2 TMG hat ergeben, dass sich hieraus nicht die generelle Unanwendbarkeit der Haftungsbeschränkung gemäß § 10 TMG auf Ansprüche der Störerhaftung gegen Betreiber von Web 2.0-Diensten

1334 *Spindler,* in: *Spindler/Schmitz/Geis,* TDG, 2004, TDG § 11 Rn. 11.
1335 Vgl. 8. Kapitel, Teil C.I.3.c.aa.(1).

ergibt.[1336] Die Regelung lässt lediglich einzelfallbezogene hoheitliche Anordnungen gegen die ISPs zu, die auf die Entfernung oder Sperrung einer konkreten, bereits eingetretenen Rechtsverletzung gerichtet sind. Dies bedeutet jedoch, dass auch negatorische Ansprüche gegen Web 2.0-Dienste, insbesondere soweit sich diese auf die Verhinderung zukünftiger Rechtsverletzungen beziehen, grundsätzlich ausgeschlossen sind. Da die Betreiber von Web 2.0-Diensten somit nicht Störer sind und ihnen keinen besonderen Prüfpflichten in Bezug auf das in ihren Internetdiensten vorhandene Material obliegen, ist auch für eine Verpflichtung der ISPs zum Einsatz von Content-Identification-Technologien grundsätzlich kein Raum. Einer solchen Verpflichtung würde darüber hinaus der Ausschluss allgemeiner Überwachungspflichten gemäß § 7 Abs. 2 S. 1 TMG entgegenstehen. Als Ergebnis bleibt somit festzuhalten, dass der Betreiber eines Web 2.0-Dienstes, sofern er die Tatbestandsvoraussetzungen gemäß § 10 TMG erfüllt, unabhängig von dem Einsatz von Content-Identification-Technologien grundsätzlich nicht als Störer haftet, und lediglich aufgrund von § 7 Abs. 2 S. 2 TMG zur Beseitigung von Rechtsverletzungen in Einzelfällen herangezogen werden kann.

3. Ergebnis

Nachfolgend werden die für die deutsch-europäische Rechtslage gefundenen Ergebnisse zusammengefasst und kritisch gewürdigt.

a. Auswirkungen von Content-Identification-Technologien auf die Haftung von Web 2.0-Diensten nach deutsch-europäischem Recht

Aufgrund der grundsätzlichen Anwendbarkeit von § 10 TMG auf urheberrechtliche Schadensersatzansprüche scheiden solche Ansprüche gegen Web 2.0-Dienste regelmäßig aus. Auf dieses Ergebnis hat weder der Einsatz von Content-Identification-Technologien noch der bewusste Verzicht hierauf einen Einfluss.

Das gleiche Ergebnis ergibt sich in Bezug auf Ansprüche der Störerhaftung wegen Urheberrechtsverletzungen, sofern man § 7 Abs. 2 S. 2 TMG entsprechend der Intention des europäischen Gesetzgebers auslegt. Hieraus ergibt sich, dass Web 2.0-Dienste durch § 10 TMG grundsätzlich auch von Ansprüchen der Störerhaftung befreit werden und § 7 Abs. 2 S. 2 TMG insoweit nur erlaubt, dass ISPs eng begrenzte, einzelfallbezogene Maßnahmen zur Beseitigung einer konkreten Rechtsverletzung auferlegt werden können. Einer darüber hinausgehenden Verpflichtung von ISPs dahingehend, Content-Identification-Technologien generell zur Verhin-

1336 Vgl. 8. Kapitel, Teil C.I.2.d.bb.

derung bzw. Beseitigung von Rechtsverletzungen einzusetzen, steht der Ausschluss allgemeiner Überwachungspflichten somit entgegen.

Folgt man in Bezug auf Ansprüche der Störerhaftung gegen einen ISP hingegen der Rechtsprechung des BGH zu Internetversteigerungen, ist § 10 TMG hierauf nicht anwendbar und haftet somit der Betreiber eines Web 2.0-Dienstes ohne Einschränkung als Störer, falls er die ihm im Zusammenhang mit ihm bekannt gewordenen Rechtsverletzungen obliegenden Prüfpflichten verletzt. Aufgrund der Ausweitung der Haftung von ISPs auf „kerngleiche" und zukünftige Rechtsverletzungen sowie der daraus erkennbaren Tendenz des BGH, im Angebot von Internetdiensten generell die Eröffnung einer Gefahrenquelle zu sehen, die besondere Schutzpflichten des ISPs in Bezug auf die Rechtspositionen Dritter nach sich zieht, ist davon auszugehen, dass ISPs auf Grundlage dieser Rechtsprechung zukünftig auch zum Einsatz von Content-Identification-Technologien verpflichtet werden dürften.

b. Bewertung

Aus diesem Ergebnis geht hervor, dass der europäische und der deutsche Gesetzgeber das Ziel, mit den Regelungen über die Haftung von Host-Providern gemäß Art. 14 Abs. 3 ECRL bzw. § 10 TMG einen interessengerechten, leicht handhabbaren, entwicklungsfähigen und flexiblen Rechtsrahmen zu schaffen, nicht erreicht haben.[1337]

Wie dargelegt wurde, beruht die Konzeption der Haftungsbeschränkungen auf der Annahme, dass eine technische Kontrolle des innerhalb von Internetdiensten stattfindenden Datenverkehrs für ISPs praktisch unmöglich ist. Daher wurde die Haftung von ISPs insoweit weitgehend beschränkt und zudem eine Verpflichtung von ISPs, ihre Internetdienste auf Rechtsverletzungen zu überwachen, gesetzlich ausgeschlossen, um zu vermeiden, dass den ISPs objektiv unerfüllbare Pflichten auferlegt werden würden. Diese den Haftungsbeschränkungen sämtlich zugrundeliegende Annahme der faktisch unmöglichen Kontrolle wurde jedoch weder in den Regelungen der ECRL noch des TMG ausdrücklich verankert. Da somit ISPs nach der Gesetzeslage zur Überwachung ihrer Dienste unabhängig davon, ob ihnen eine solche Überwachung technisch möglich wäre, nicht verpflichtet sind, bestehen ihrerseits keinerlei Anreize, vorhandene Technologien, die eine verbesserte Überwachung von Internetdiensten auf rechtsverletzendes Material und damit einen besseren Schutz von Urheberrechten ermöglichen würden, einzusetzen. Denn auf die Beschränkung ihrer Haftung wirkt sich die Ergreifung solcher Maßnahmen,

1337 *Marly*, in: *Grabitz/Hilf/Nettesheim* (Hrsg.), EU, 2009, A 4, Art. 12 Rn. 7.

deren Implementierung zudem mit erheblichem zeitlichen, technischen und finanziellen Aufwand verbunden ist, nicht aus. Zwar hätte eine Regelung, die die Anwendbarkeit der Haftungsbeschränkung davon abhängig macht, dass der ISP alle Mittel einsetzt, um Urheberrechte im Rahmen des zum jeweiligen Zeitpunkt technisch Möglichen und Zumutbaren zu schützen, weniger Rechtssicherheit bedeutet. Denn der Umfang der Beschränkung der Haftung von ISPs hätte demnach unter anderem von zukünftigen technischen Entwicklungen abgehangen. Andererseits hätte eine solche Regelung mehr Möglichkeiten geboten, auf die im Vorhinein zumeist nicht absehbaren neuen technischen Entwicklungen im Bereich des Internets flexibler zu reagieren.[1338]

Vor diesem Hintergrund erscheint daher die vom BGH entwickelte Lösung fast vorzugswürdig.[1339] Denn hierdurch kann im Rahmen der Prüfung der Prüfpflichtverletzung unter Berücksichtigung der im jeweiligen Zeitpunkt und nach den konkreten Umständen verfügbaren technischen Möglichkeiten für jeden Einzelfall eine angemessene Lösung gefunden werden. Für diesen Ansatz spricht auch, dass aufgrund neuer technischer Entwicklungen wie beispielsweise Content-Identification-Technologien die Kontrolle von Datenströmen im Internet in gewissem Umfang möglich wird. Damit wird jedoch die Rechtfertigung des Anspruchs von ISPs auf eine Beschränkung ihrer Haftung zunehmend in Frage gestellt.[1340] Aufgrund dieser Entwicklung rücken ISPs nach und nach in die Position eines „normalen" Anbieters von Produkten oder Dienstleistungen in der analogen Welt heran, der in der Regel für seine Tätigkeiten und die daraus für die Rechtspositionen Dritter resultierenden Gefahren keine speziellen Haftungserleichterungen genießt. Gerade im deutschen

1338 Ähnlich sieht es auch *Spindler*, MMR 2007, 511, 514: Der Kern des Problems im Zusammenhang mit den Haftungsbeschränkungen des TMG liege in der Frage, ob unter Effizienzgesichtspunkten am ehesten der Rechtsinhaber oder der Provider eine Rechtsverletzung überwachen oder verfolgen kann. Die Lösung könne nicht ein „Schwarz-Weiß" sein, sondern nur ein Mittelweg, bei dem sowohl Anreize zum Einsatz von Überwachungssystemen zur Rechtsüberwachung gesetzt als auch Risiken für Provider minimiert werden.

1339 So äußerte sich auch die derzeitige Bundesjustizminsterin *Sabine Leutheusser-Schnarrenberger* in ihrer „Berliner Rede zum Urheberrecht" vom 14.06.2010: *„Ich meine, die Rechtsprechung des Bundesgerichtshofs sichert einen fairen Ausgleich der Interessen, indem sie den Rechteinhabern unter bestimmten Voraussetzungen einen Beseitigungs- und Unterlassungsanspruch auch gegenüber dem Provider zuerkennt. Nämlich dann, wenn dieser seine Prüfpflichten nicht erfüllt und es ihm im Einzelfall möglich und zumutbar ist, die Rechtsverletzung zu verhindern. Auch wenn dies manche fordern, halte ich es nicht für richtig, diese Rechtslage zum Nachteil der Rechteinhaber zu verändern. Die Provider bleiben hier in der Verantwortung."* Die Rede ist abrufbar unter http://www.bmj.bund.de/enid/0,41c20c636f6e5f6964092d0936393139093a095f7472636964092d0936393230/Reden/Sabine_Leutheusser-Schnarrenberger_1mt.html (zuletzt abgerufen am 01.07.2010).

1340 *Rössl/Rössl*, CR. 2005, 809, 815; so auch *Lehmann*, CR 1998, 233, 234, der bereits sehr früh die weitreichenden Haftungsbeschränkungen für Provider als „rechtspolitisch verfehlt" qualifizierte: *„Die Rechtsgeschäfte im Netz ... benötigen Rechtssicherheit, aber nicht eine wirtschaftspolitisch falsch verstandene Standortsubventionierung durch Haftungsbeschränkung."*

Recht ist es zudem Tradition, dass für Gefahren, die sich aus neuen Technologien ergeben, grundsätzlich der Nutznießer dieser Technologien einstehen muss, beispielsweise im Rahmen einer verschuldensunabhängigen Gefährdungshaftung.[1341] Auch sollte es grundsätzlich Aufgabe des Rechts sein, Anreize dafür zu bieten, dass verfügbare technische Mittel zur Eindämmung der missbräuchlichen Verwendung von Produkten und Dienstleistungen nach Möglichkeit genutzt werden.[1342]

II. Rechtsvergleich

Auf der Grundlage der gefundenen Ergebnisse zur Haftung von ISPs, die Web 2.0-Dienste betreiben, innerhalb derer die Nutzer Rechtsverletzungen begehen, sowie zu den Auswirkungen von Content-Identification-Technologien hierauf, wird nachfolgend die bestehende Rechtslage nach US-amerikanischem und deutsch-europäischem Urheberrecht verglichen. Dabei werden zunächst allgemein die Gemeinsamkeiten und Unterschiede der materiell-rechtlichen Haftung von Web 2.0-Diensten sowie der Haftungsbeschränkung für Host-Provider dieser Jurisdiktionen dargestellt. Auf dieser Grundlage wird im Anschluss verglichen, welche Konsequenzen in haftungsrechtlicher Sicht die Verfügbarkeit von Content-Identification-Technologien nach sich zieht.

1. Vergleich der Rechtslage betreffend die materiell-rechtliche Haftung von Web 2.0-Diensten

Auf der Ebene der Haftungsbegründung bestehen erhebliche Unterschiede zwischen der US-amerikanischen und der deutsch-europäischen Rechtslage.

Nach US-amerikanischem Recht bleibt die Haftung von ISPs dem Grunde nach, d.h. nach den Grundsätzen der *primary* und der *secondary liability*, von der Haftungsbeschränkung gemäß § 512(c) unberührt. Dies bedeutet, dass es für die Beurteilung der Haftung von ISPs nach diesen Grundsätzen zunächst keine Rolle spielt, ob die Haftungsbeschränkung gemäß § 512(c) auf den ISP Anwendung findet. Denn die Voraussetzungen der einschlägigen Rechtsinstitute werden durch § 512(c) nicht überlagert oder modifiziert. Vielmehr beschränkt die Haftungsbeschränkung im Falle ihres Eingreifens lediglich die Folgen der dem Grunde nach bestehenden urheberrechtlichen Primär- oder Sekundärhaftung des ISPs für die Rechtsverletzungen der Nutzer seines Internetdienstes.

1341 *Lehmann*, in: *Lehmann/Meents* (Hrsg.), FA IT-Recht, Kap. 10, Rn. 11.
1342 *Rössl/Rössl*, CR 2005, 809, 815; *Lehmann*, ZUM 1999, 180, 183.

Allerdings scheidet eine Haftung von ISPs als *primary infringer* in der Regel bereits nach den Grundsätzen von *Netcom* aus. Demnach gelten als unmittelbare Täter von Urheberrechtsverletzungen, die in Bezug auf urheberrechtlich geschützte Multimediawerke innerhalb von Internetdiensten begangen werden, grundsätzlich nur die Nutzer. Der ISP kann für deren Handlungen nach *Netcom* als *primary infringer* nur im Falle des Hinzutretens weiterer Umstände („volition" oder „causation") haftbar gemacht werden. Darüber hinaus kommt im US-amerikanischen Recht jedoch eine Haftung des ISPs als *secondary infringer* nach den Grundsätzen des *contributory infringement* oder der *vicarious liability* in Betracht. Die Analyse der einzelnen Voraussetzungen dieser beiden Rechtsinstitute hat gezeigt, dass ein ISP, der im Rahmen seines Internetdienstes Content-Identification-Technologien einsetzt, aufgrund dieser Tatsache Gefahr läuft, wegen des Bestehens einer tatsächlichen Beherrschungsmöglichkeit in Bezug auf das rechtswidrige Verhalten der Nutzer als *vicarious infringer* haftbar gemacht zu werden. Hingegen kann auf die Tatsache, dass ein ISP Content-Identification-Technologien nicht einsetzt, die Haftung des ISPs als *contributory infringer* gestützt werden, sofern man insoweit für das subjektive Erfordernis der *constructive knowledge* ein bewusstes Sichverschließen vor Kenntnis ausreichen lässt. Denn ein solches bewusstes Sichverschließen kann darauf gestützt werden, dass es der ISP in seiner Eigenschaft als *cheapest cost avoider* unterläßt, Urheberrechtsverletzungen durch Einsatz technischer Mittel nach Möglichkeit einzudämmen, ohne hierfür zwingende (wirtschaftliche) Gründe nennen zu können. Weiterhin birgt der Nichteinsatz von Content-Identification-Technologien für den ISP das Risiko, dass dieser deswegen auch nach der *inducement rule* als *contributory infringer* haftet. Nach der gegenwärtigen US-amerikanischen Rechtslage lässt sich somit die materiell-rechtliche Haftung sowohl gegenüber einem ISP, der Content-Identification-Technologien einsetzt, als auch gegen einen ISP, der hierauf bewußt verzichtet, begründen. Aus materiell-rechtlichen Gesichtspunkten ist es somit im Ergebnis gleichgültig, ob sich ein ISP für oder gegen Content-Identificiation-Technologien in seinem Internetdienst entscheidet, da sich jede Entscheidung auf seine materiell-rechtliche Haftung sowohl positiv als auch negativ auswirken kann.

Währenddessen kommen nach deutsch-europäischem Urheberrecht gegen ISPs materiell-rechtliche Ansprüche in Form des urheberrechtlichen Schadensersatzanspruches gemäß § 97 Abs. 2 S. 1 UrhG sowie Unterlassungs- und Beseitigungsansprüche der urheberrechtlichen Störerhaftung in Betracht. Allerdings ist nach deutsch-europäischem Recht für das Bestehen dieser materiell-rechtlichen Ansprüche entscheidend, ob die auf Art. 14 ECRL basierende Haftungsbeschränkung gemäß § 10 TMG eingreift. Denn aufgrund der dogmatischen Einordnung der Haftungsbeschränkung als „tatbestandsintegrierter Vorfilter" werden hierdurch anders als im US-amerikanischen Recht nicht nur die Haftungsfolgen, sondern vielmehr

die tatbestandliche Reichweite einer Haftungsnorm beschränkt. Damit wirkt sich § 10 TMG auf der Ebene der materiell-rechtlichen Begründung der Haftung des ISPs aus, d.h. werden im Falle der Anwendbarkeit dieser Vorschrift Ansprüche gegen den ISP bereits dem Grunde nach ausgeschlossen.

Als Ergebnis bleibt somit festzuhalten, dass ein Web 2.0-Dienst nach US-amerikanischem Recht unabhängig von dem Eingreifen der Haftungsbeschränkung gemäß § 512(c) zunächst als *primary* oder *secondary infringer* haften kann. Sofern § 512(c) eingreift, wird der ISP hierdurch nur vor den Folgen einer solchen Haftung geschützt. Hingegen ist nach deutsch-europäischem Recht im Falle des Eingreifens der Haftungsbeschränkung gemäß § 10 TMG eine Urheberrechtsverletzung seitens des ISPs bereits tatbestandlich ausgeschlossen.

2. Vergleich der Haftungsbeschränkungen für Host-Provider gemäß § 512(c) bzw. § 10 TMG

Sowohl nach US-amerikanischem als auch nach deutsch-europäischem Recht hängt die Haftung von ISPs im Ergebnis davon ab, ob die jeweilige Haftungsbeschränkung für Host-Provider – gemäß § 512(c) bzw. Art. 14 ECRL/§ 10 TMG – eingreift. Gemeinsamkeiten und Unterschiede dieser Regelungen werden nachfolgend dargestellt.

a. Gemeinsamkeiten: gleiche Motivation hinter der Einführung der Haftungsbeschränkungen

Die US-amerikanische und die deutsch-europäische Haftungsbeschränkung basieren auf identischen Erwägungen. Einerseits soll mit ihrer Hilfe der sich im Internet entwickelnde elektronische Geschäftsverkehr einschließlich der damit einhergehenden neuen Geschäftsmodelle, Technologien und Kommunikationswege befördert werden. Denn durch die Haftungsbeschränkungen soll zugunsten der ISPs, die solche Produkte und Dienstleistungen anbieten, Rechtssicherheit betreffend die Voraussetzungen und den Umfang ihrer Haftung für Rechtsverletzungen, die Nutzer innerhalb ihrer Internetdienste begehen, geschaffen werden. Zu diesem Zweck werden ISPs unter bestimmten Voraussetzungen von der Haftung für rechtswidrige Aktivitäten innerhalb ihrer Internetdienste weitgehend befreit. Die Haftungsbeschränkungen beruhen weiterhin auf der Annahme, dass ISPs eine Kontrolle des innerhalb ihrer Internetdienste automatisch abgewickelten Datenverkehrs technisch nicht möglich ist und deswegen eine Haftung ihrerseits insoweit nicht gerechtfertigt wäre. Daher dürfen ISPs gemäß § 512(m) bzw. 15 Abs. 1 ECRL/§ 7

Abs. 2 S. 1 TMG nicht zur aktiven Überwachung ihrer Internetdienste verpflichtet werden.

Andererseits sollen auch die Interessen der Rechtsinhaber an der Beseitigung und Verhinderung von im Internet stattfindenden Eingriffen in ihre Rechtspositionen angemessen berücksichtigt werden. Daher sehen sowohl § 512(j) als auch Art. 14 Abs. 3 ECRL/§ 7 Abs. 2 S. 2 TMG vor, dass ISPs ungeachtet des Eingreifens der jeweiligen Haftungsbeschränkung weiterhin zur Beseitigung konkreter Rechtsverletzungen durch hoheitliche Maßnahmen verpflichtet werden können.

b. Unterschiede

Im Übrigen bestehen jedoch erhebliche Unterschiede in Bezug auf die konkrete Ausgestaltung der Haftungsbeschränkungen.

aa. Reichweite der Haftungsbeschränkungen

Ein wesentlicher Unterschied besteht zunächst im Hinblick auf die Reichweite der Haftungsbeschränkungen. So beschränkt § 512(c) die Haftung von ISPs lediglich in Bezug auf *copyright infringement*. Dies bedeutet, dass die Haftung von ISPs für alle anderen Bereiche außerhalb des Urheberrechts hiervon unberührt bleibt. Hingegen wird durch § 10 TMG die Haftung von ISPs „horizontal" beschränkt, d.h. rechtsgebietsübergreifend und damit unabhängig davon, ob die jeweilige Haftungsnorm dem Zivil-, Straf- oder öffentlichen Recht angehört. § 10 TMG befreit somit im Falle des Eingreifens dieser Regelung einen ISP nicht nur von der urheberrechtlichen Haftung, sondern darüber hinaus von jeglicher zivilrechtlicher, strafrechtlicher oder öffentlich-rechtlicher Verantwortlichkeit.

bb. Folgen des Eingreifens der Haftungsbeschränkungen

Ein wesentlicher Unterschied besteht weiterhin in der gesetzlichen Ausgestaltung der Rechtsfolgen, die sich aus dem Eingreifen der Haftungsbeschränkungen ergeben.

Die haftungsrechtlichen Folgen des Eingreifens von § 512(c) sind klar gesetzlich geregelt. So geht aus dem Wortlaut von § 512(c) hervor, dass hierdurch jegliche finanzielle Entschädigungsansprüche („monetary relief") gegen den ISP ausgeschlossen werden. Darüber hinaus werden in § 512(j) Art und Umfang des Erlasses von *injunctions* geregelt. Die Möglichkeiten der Gerichte, gegen ISPs solche Hand-

lungs- oder Unterlassungsverfügungen zu erlassen, werden stark eingeschränkt und an bestimmte, gesetzlich geregelte Voraussetzungen geknüpft. Diese klaren Regelungen betreffend den Umfang der Haftung des ISPs im Falle des Eingreifens der Haftungsbeschränkung werden ergänzt durch das Notice&Takedown-Verfahren gemäß § 512(c)(3). Hierdurch wird den Rechtsinhabern eine attraktive Alternative zur Beseitigung von Rechtsverletzungen unabhängig von der materiellrechtlichen Inanspruchnahme des ISPs geboten, in Form eines klar geregelten Mechanismus zur Beseitigung bereits eingetretener Rechtsverletzungen.

Hingegen besteht nach der deutschen-europäischem Rechtslage gemäß § 10 TMG lediglich Klarheit darüber, dass jedenfalls verschuldensabhängige deliktische und strafrechtliche Ansprüche gegen den ISP im Falle des Eingreifens der Haftungsbeschränkung vollumfänglich ausgeschlossen sind. Weitgehende Rechtsunsicherheit besteht jedoch darüber, inwieweit ein ISP trotz der Anwendbarkeit von § 10 TMG als Störer haftbar gemacht werden kann, d.h. Beseitigungs- und Unterlassungsansprüchen in Bezug auf die innerhalb seines Internetdienstes begangenen Rechtsverletzungen ausgesetzt ist. Da die ECRL insoweit keine eindeutigen Vorgaben außer der Öffnungsklausel gemäß Art. 14 Abs. 3 ECRL enthält, herrscht hierüber im Anwendungsbereich von § 10 TMG weitgehende Rechtsunsicherheit, die in der BGH-Rechtsprechung zu Internetversteigerungen sowie in der darauf folgenden Instanzrechtsprechung ihren Niederschlag gefunden hat, wonach § 10 TMG grundsätzlich nicht auf negatorische Ansprüche anwendbar ist. Dies bedeutet jedoch, dass nach deutsch-europäischem Recht ISPs dieser Haftung, die gerade im Bereich des Urheberrechts eine wichtige Rolle spielt, weiterhin vollumfänglich ausgesetzt sind. ISPs können daher in Bezug auf bekannte und nach der Rechtsprechung des BGH darüber hinaus auch für damit kerngleiche sowie erst zukünftig zu erwartende Rechtsverletzungen als Störer haftbar gemacht werden, sofern sie die ihnen ab Kenntnis von einer Rechtsverletzung obliegenden Prüfpflichten verletzen.

cc. Subjektive Voraussetzungen der Anwendbarkeit

Weiterhin unterscheiden sich die US-amerikanische und die deutsch-europäische Haftungsbeschränkung in Bezug auf die subjektiven Voraussetzungen, die zu einem Verlust des Anspruchs auf die Haftungsbeschränkung seitens des ISPs führen.

Zwar muss sowohl bei § 512(c)(1)(A) als auch bei § 10 TMG sich die Kenntnis des ISPs gerade auch auf die Rechtswidrigkeit des betreffenden Materials oder der Tätigkeit eines Nutzers beziehen. Allerdings reicht gemäß § 10 S. 1 Nr. 1 TMG neben positiver Kenntnis bereits „normale“ grob fahrlässige Unkenntnis des ISPs von der Rechtswidrigkeit der Information oder Handlung zum Verlust der Haf-

tungsbeschränkung in Bezug auf Schadensersatzansprüche aus. Hingegen führt im Rahmen von § 512(c)(1)(A) neben der positiven Kenntnis nur das Bewusstsein von *red flags*, d.h. von Umständen, aus denen die Rechtswidrigkeit des Materials oder der Handlung offensichtlich hervorgeht, zur Unanwendbarkeit der Haftungsbeschränkung. Wie gezeigt wurde, genügen dieser Anforderung nur Umstände, bei denen deutliche Hinweise auf eklatante Rechtsverletzungen vorliegen, d.h. die Rechtswidrigkeit dem Material oder der Handlung gleichsam „auf die Stirn geschrieben" ist. Allerdings führt das Bewusstsein von *red flags* nicht nur zum Verlust der Haftungsbeschränkung in Bezug auf Schadensersatzansprüche, sondern in Bezug auf sämtliche Ansprüche, die sich aus einer Urheberrechtsverletzung ergeben können.

dd. US-amerikanische Ausschlusskriterien ohne direktes Pendant im deutsch-europäischen Recht

Die US-amerikanische Haftungsbeschränkung stellt über die subjektiven Voraussetzungen hinaus noch zwei weitere Anforderungen an einen ISP, die dieser erfüllen muss, um den Schutz gemäß § 512(c) für sich beanspruchen zu können. Hingegen stellt die deutsch-europäische Regelung gemäß § 10 TMG keine weiteren Anforderungen an ihre Anwendbarkeit, außer dass der die Rechtsverletzung unmittelbar begehende Nutzer nicht der Aufsicht des ISPs unterstellt sein darf.

(1) Unmittelbarer wirtschaftlicher Vorteil bei gleichzeitigem Vorliegen der rechtlichen und tatsächlichen Beherrschungsmöglichkeit in Bezug auf das rechtswidrige Verhalten

Gemäß § 512(c)(1)(B) darf ein ISP, der über eine rechtliche und tatsächliche Beherrschungsmöglichkeit in Bezug auf das urheberrechtswidrige Verhalten der Nutzer verfügt, keinen unmittelbaren wirtschaftlichen Vorteil aus diesem Verhalten ziehen. Die Einführung dieses Ausschlusskriteriums ist konsequent in Anbetracht der Tatsache, dass eine der grundlegenden Annahmen, auf der die Einführung der Haftungsbeschränkungen für ISPs sowohl im US-amerikanischen als auch im deutsch-europäischen Recht beruht, die fehlende Kontrolle der ISPs über den innerhalb ihrer Internetdienste stattfindenden Datenverkehr ist. Vor diesem Hintergrund ist es folgerichtig, den Schutz der Haftungsbeschränkung entfallen zu lassen, wenn der ISP entgegen dieser Annahme dennoch über eine solche Kontrollmöglichkeit verfügt und aus dem von ihm faktisch beherrschbaren rechtswidrigen Verhalten einen unmittelbaren wirtschaftlichen Vorteil zieht. Denn hieraus kann ge-

schlossen werden, dass der ISP von den Eingriffen in fremde Urheberrechte zielgerichtet profitieren will, indem er darauf verzichtet, solches Verhalten durch Ausübung der faktischen Beherrschungsmöglichkeit zu unterbinden.

Zwar wurde dargelegt, dass die derzeitige Konzeption dieses Ausschlusskriteriums im Detail durchaus kritikwürdig und verbesserungsfähig ist,[1343] insbesondere da sich weder dem Gesetzestext noch aus den Materialien zum Gesetzgebungsverfahren ausreichende Anhaltspunkte entnehmen lassen, was unter der Voraussetzung des unmittelbaren wirtschaftlichen Vorteils – gerade im Kontext der oftmals werbebasierten neuen Geschäftsmodelle des E-Commerce – im Einzelnen zu verstehen ist. Demgegenüber erscheint es jedoch als das größere Versäumnis, dass der europäische Gesetzgeber ein solches Ausschlusskriterium in die Haftungsbeschränkung gemäß Art. 14 ECRL erst gar nicht aufgenommen hat. Denn dadurch fehlt es im deutsch-europäischen Recht an einem Ansatzpunkt, um einen ISP vom Anwendungsbereich der Haftungsbeschränkung auszuschließen, wenn aus den Umständen hervorgeht, dass dieser sein Geschäftsmodell bewusst so ausgestaltet hat, dass er Rechtsverletzungen trotz bestehender Einwirkungsmöglichkeiten geschehen lässt, um hiervon wirtschaftlich zu profitieren, solange ihm nicht grob fahrlässige Unkenntnis von einer konkreten Rechtsverletzung nachgewiesen werden kann. Aufgrund des Ausschlusses allgemeiner Überwachungspflichten kann eine solche grobe Fahrlässigkeit auch nicht über den Verzicht des ISPs auf die Ergreifung von proaktiven Maßnahmen zur Verhinderung von Rechtsverletzungen gestützt werden.

Möglicherweise hat jedoch der EuGH in seiner Entscheidung vom 23.03.2010, in der es um die Haftung von Google für dessen Referenzierungsdienst ging, also die Zuschaltung von Werbung zu Suchergebnissen auf Grundlage bestimmter „Schlüsselworte", bereits einen möglichen Ausweg aus dem deutsch-europäischen Dilemma aufgezeigt.[1344] Darin hat das Gericht festgehalten, dass für die Feststellung, ob die Verantwortlichkeit eines ISPs aufgrund Art. 14 ECRL beschränkt ist, zu prüfen ist, „ob die Rolle dieses Anbieters [des ISPs] insofern neutral ist, als sein Verhalten rein technischer, automatischer und passiver Art ist und er weder Kenntnis noch Kontrolle über die weitergeleitete oder gespeicherte Information besitzt."[1345] Damit wurde jedoch für die Auslegung von Art. 14 ECRL auf das Verhalten eines ISPs der 42. Erwägungsgrund der ECRL für unmittelbar maßgeblich erklärt. Demnach sind für die Anwendbarkeit der in der ECRL festgelegten Aus-

1343 Vgl. 8. Kapitel, Teil B.IV.3.a.bb.

1344 EuGH vom 23.03.2010, Rs. C-236/08 bis C 238/08, Google France/Louis Vuitton; vgl. hierzu die Besprechung von *Fitzner*, MMR 2010, 83.

1345 EuGH vom 23.03.2010, Rs. C-236/08 bis C 238/08, Google France/Louis Vuitton, Rz. 114; in einem obiter dictum hat der BGH diese vom EuGH postulierte (zusätzliche) Voraussetzung der Anwendbarkeit der Haftungsbeschränkungen auf ISPs bereits übernommen, vgl. BGH vom 29.04.2010, GRUR 2010, 628, 639 (Rn. 39) - Vorschaubilder.

nahmen der Verantwortlichkeit von ISPs genau diese Kriterien der Kenntnis und Kontrolle ausschlaggebend. Damit wird jedoch einer Argumentation die Tür geöffnet, wonach das Verhalten des ISPs über die gesetzlich ausformulierten Tatbestandsmerkmale hinaus einer wertenden Gesamtbetrachtung zu unterziehen ist und im Ergebnis der Schutz der Haftungsbeschränkungen nur einem ISP gewährt werden darf, dessen Verhalten keinerlei Hinweise darauf gibt, dass er das rechtswidrige Verhalten der Nutzer kontrollieren kann. Denn wenn eine solche faktische Kontrolle des ISPs besteht, würde nach der Lesart des EuGH die grundsätzliche Voraussetzung und Rechtfertigung für die Beschränkung der Haftung des ISP entfallen.

(2) Standard Technical Measures

Darüber hinaus sieht die US-amerikanische Regelung in § 512(i)(1)(B) vor, dass die Haftungsbeschränkung auf einen ISP nicht anwendbar ist, wenn dieser im Rahmen seines Internetdienstes keine Technologien einsetzt, die als STMs zu qualifizieren sind. Zudem bilden STMs eine Ausnahme von dem Ausschluss allgemeiner Überwachungspflichten, indem ISPs zur Überwachung ihrer Internetdienste auf Rechtsverletzungen insoweit verpflichtet werden können, als solche Maßnahmen durch STMs ermöglicht werden.

Zwar ist wiederum die konkrete Ausgestaltung dieses *threshold requirements*, insbesondere die Definition des Begriffs der STMs, wie dargelegt wurde, kritikwürdig,[1346] jedoch ist der Zweck, der mit dieser Regelung verfolgt wird, ohne Einschränkung zu begrüßen. Denn die durch die Haftungsbeschränkungen geschaffene Sonderstellung der ISPs in Bezug auf die Haftung für Urheberrechtsverletzungen kann nur solange und soweit Geltung beanspruchen, wie die technische Beschaffenheit und die damit einhergehenden Kontroll(un)möglichkeiten der Internetdienste der ISPs dies rechtfertigen. Wenn jedoch die Kontrolle des Datenverkehrs in Internetdiensten durch neue technologische Entwicklungen, wie beispielsweise durch Content-Identification-Technologien, zumindest in gewissem Umfang möglich wird, müssen die Haftungsbeschränkungen auf diesen Umstand entsprechend reagieren können. Die Einführung einer Verpflichtung von ISPs, neue Technologien, die eine bessere Kontrolle von Urheberrechtsverletzungen ermöglichen, einsetzen zu müssen, wenn sie die Vorteile der Haftungsbeschränkung weiterhin für sich beanspruchen wollen, wie sie § 512(i)(1)(B) eigentlich vorsehen möchte, stellt eine solche Reaktionsmöglichkeit dar.

Hingegen fehlt im deutsch-europäischen Recht eine solche Reaktionsmöglichkeit gänzlich. Damit ist im Anwendungsbereich von Art. 12-15 ECRL bzw. §§ 7-10

1346 Vgl. 8. Kapitel, Teil B.IV.3.a.aa.

TMG jedoch die Annahme der technischen Unmöglichkeit von Kontroll- und Überwachungsmaßnahmen in Bezug auf Rechtsverletzungen, die innerhalb von Internetdiensten stattfinden, für alle Zukunft unabhängig von den tatsächlichen technischen Entwicklungen gleichsam „einbetoniert". Technische Neuerungen, die die Privilegierung von ISPs mit der Begründung fehlender tatsächlicher Kontrollmöglichkeiten grundsätzlich in Frage stellen, können somit innerhalb der Prüfung der Anwendbarkeit der Haftungsbeschränkung nicht angemessen berücksichtigt werden. Dies führt zwangsläufig zu Ergebnissen, die nicht interessengerecht sind. Denn auf diese Weise kann ein ISP, der innerhalb seines Internetdienstes stattfindende Rechtsverletzungen technisch kontrollieren könnte, hierauf aber bewusst verzichtet, dennoch in den Genuß der Haftungsbeschränkung gemäß § 10 TMG kommen. Damit wird der ISP jedoch in seiner Haftung privilegiert, obwohl er die Grundannahme, auf der die Gewährung dieses Privilegs basiert nicht mehr erfüllt, nämlich die technische Unmöglichkeit der Kontrolle des Datenverkehrs. Einen Ausweg aus diesem Dilemma könnte nur der vom EuGH bereits angedeutete unmittelbare Rückgriff auf den 42. Erwägungsgrund der ECRL weisen, wonach die fehlende Kontrolle eine zusätzliche Voraussetzung für die Anwendbarkeit der Haftungsbeschränkungen ist.

ee. Ergebnis

Im Vergleich mit der deutsch-europäischen Haftungsbeschränkung gemäß Art. 14 ECRL/§ 10 TMG erscheint § 512(c) insgesamt als die überzeugendere Regelung. Denn zum einen schafft § 512(c) tatsächlich Rechtssicherheit über die Voraussetzungen und den Umfang der Haftung von ISPs in Bezug auf die innerhalb ihrer Internetdienste durch die Nutzer begangenen Urheberrechtsverletzungen. Denn § 512 regelt mit aller Klarheit die Rechtsfolgen, denen sich ein ISP im Falle der Anwendbarkeit einer der Safe-Harbor-Regelungen noch ausgesetzt sehen kann, vor allem auch im Hinblick auf *injunctions*. Hingegen besteht im deutsch-europäischen Recht trotz der Einführung der Haftungsbeschränkungen nach wie vor weitgehende Rechtsunsicherheit über den Umfang der Haftung von ISPs. Dies hat zu der Rechtsprechung des BGH geführt, wonach die im Urheberrecht eine herausragende Rolle spielende Störerhaftung auf ISPs weiterhin vollumfänglich Anwendung findet. Unterlassungs- und Beseitigungsansprüche gegen ISPs sind damit unverändert von der einzelfallabhängigen Bestimmung der Zumutbarkeit von Prüfpflichten abhängig.

Auch berücksichtigt nur die US-amerikanische Regelung ausreichend die Umstände, die zu einem Entfallen der Haftungsbeschränkung zugunsten von ISPs führen müssen. Denn da sowohl § 512(c) als auch Art. 12 ECRL/§ 10 TMG auf der

Annahme basieren, dass ISPs die rechtswidrigen Aktivitäten der Nutzer innerhalb ihrer Internetdienste technisch nicht kontrollieren können und ihnen daher eine Überwachung ihrer Dienste auf Rechtsverletzungen grundsätzlich nicht zumutbar ist, müssen diese Regelungen den Fall berücksichtigen, dass sich diese Annahme überholt. Für diesen Fall sieht das US-amerikanische Recht vor, dass ISPs speziell den Schutz der Haftungsbeschränkung gemäß § 512(c) dann verlieren, wenn sie das Verhalten der Nutzer kontrollieren können und darüber hinaus von diesen Handlungen bewusst wirtschaftlich profitieren. Weiterhin ist die Anwendbarkeit von § 512(c) von vornherein ausgeschlossen, wenn der ISP STMs in seinem Internetdienst nicht einsetzt. Ferner kann ein ISP im Zusammenhang mit STMs auch zu einer Überwachung seines Internetdienstes verpflichtet werden, soweit dies durch STMs tatsächlich ermöglicht wird.

Hingegen sieht das deutsch-europäische Konzept neben den subjektiven Tatbestandsvoraussetzungen gemäß § 10 S. Nr. 1 TMG keine solchen speziellen Gründe vor, die zum Verlust des Anspruchs auf die Haftungsbeschränkung führen können. Damit besteht der Anspruch auf die Haftungsbeschränkung grundsätzlich auch dann fort, wenn Technologien entwickelt werden, die Kontrolle des Datenverkehrs in Internetdiensten und damit die Identifikation von Rechtsverletzungen ermöglichen und damit die grundlegende Voraussetzung für die Gewährung der Haftungsbeschränkung entfällt.

3. Vergleich der Auswirkungen des (Nicht-)Einsatzes von Content-Identification-Technologien auf die Haftung von Web 2.0-Diensten

Allerdings zeigen die Ergebnisse der Prüfung, welche Auswirkungen die Verfügbarkeit von Content-Identification-Technologien auf die Haftung von Web 2.0-Diensten hat, dass insoweit weder § 512(c) noch Art. 14 ECRL/§ 10 TMG in ihrer derzeitigen Form zu einer interessengerechten Lösung führen.

a. Gegenwärtige Situation: Kontraproduktive Ergebnisse sowohl nach § 512(c) als auch gemäß § 10 TMG

Nach der US-amerikanischen Rechtslage vergrößert der Einsatz von Content-Identification-Technologien aufgrund der dadurch eröffneten Kontrollmöglichkeiten zunächst auf der Ebene der materiell-rechtlichen Haftung das Risiko des Betreibers eines Web 2.0-Dienstes, für die Urheberrechtsverletzungen der Nutzer als *vicarious infringer* haftbar gemacht zu werden. Auf der Ebene der Haftungsbeschränkung läuft ein ISP weiterhin aufgrund des Einsatzes solcher Technologien Gefahr,

deswegen den Anspruch auf den Schutz der Haftungsbeschränkung aufgrund Erfüllung des Ausschlusskriteriums gemäß § 512(c)(1)(B) zu verlieren. Im Ergebnis hat damit ein ISP, der Content-Identification-Technologien einsetzt, ein höheres Risiko, für die Urheberrechtsverletzungen seiner Nutzer haftbar gemacht zu werden als seine Konkurrenten, die keine finanziellen und technischen Ressourcen in den Einsatz einer Content-Identification-Technologie investieren. Denn letztere können nach der derzeitigen Rechtslage – trotz des Risikos der materiell-rechtlichen Haftung als *contributory infringer* – weitgehend auf den Schutz der Haftungsbeschränkung vertrauen, da diese in ihrer derzeitigen Fassung keinen Ansatzpunkt dafür bietet, dem ISP den Schutz der Haftungsbeschränkung allein aufgrund des Verzichts auf den Einsatz von Technologien, die einen verbesserten Schutz von Urheberrechten ermöglichen, zu versagen. Für dieses Ergebnis zeichnet vor allem das *threshold requirement* gemäß § 512(i)(1)(B) verantwortlich, da nach der verunglückten Legaldefintion von STMs sich Content-Identification-Technologien bisher nicht als eine solche Maßnahme qualifizieren konnten, von deren Einsatz die Anwendbarkeit der Haftungsbeschränkung von vornherein abhängen würde. Damit setzt § 512(c) ISPs jedoch nicht nur keine Anreize, solche Technologien, die einen verbesserten Schutz von Urheberrechten ermöglichen, einzusetzen, sondern schreckt hiervon sogar ab, da ein ISP mit dem Einsatz einer solchen Technologie seine Rechtsposition gegenüber seinen Konkurrenten sogar verschlechtert.

Hingegen hat die Analyse der deutsch-europäischen Rechtslage gezeigt, dass sich hier der Einsatz einer Content-Identification-Technologie weder positiv noch negativ auf die Haftung des Betreibers eines Web 2.0-Dienstes auswirkt, sofern man § 10 TMG europarechtskonform auslegt. Denn auf die Beurteilung der subjektiven Voraussetzungen gemäß § 10 S. 1 Nr. 1 TMG, deren Vorliegen zum Ausschluss der Haftungsbeschränkung führt, hat die Tatsache des (Nicht)Einsatzes von Content-Identification-Technologien keinerlei Einfluss. Auch scheidet eine Verpflichtung eines ISPs zum Einsatz von Content-Identification-Technologien aufgrund des Ausschlusses allgemeiner Überwachungspflichten gemäß § 7 Abs. 2. S. 1 TMG aus. Dies bedeutet jedoch, dass auch nach der deutsch-europäischen Rechtslage einem ISP derzeit keinerlei Anreize geboten werden, Technologien, die den Schutz von Urheberrechten innerhalb von Internetdiensten wesentlich verbessern, einzusetzen. Zu einem anderen Ergebnis kommt man insoweit nur, wenn man der – in ihrer Begründung abzulehnenden – Rechtsprechung des BGH zu Internetversteigerungen folgt. Demnach ist davon auszugehen, dass ein ISP zur Erfüllung der ihm in Bezug auf bekannte sowie damit kerngleichen Rechtsverletzungen obliegenden Prüfpflichten grundsätzlich auch Content-Identification-Technologien einsetzen muss. Allein die Rechtsprechung des BGH setzt somit einen Anreiz zum Einsatz von Content-Identification-Technologien, da der ISP nur

durch deren Einsatz sicherstellen kann, dass er ihm etwaig obliegende Prüfpflichten nicht verletzt und damit vor Ansprüchen der Störerhaftung verschont bleibt.

b. Verbesserungsvorschläge

Um ein zufriedenstellendes Ergebnis in Bezug auf die Auswirkungen von Content-Identification-Technologien auf die Haftung von Web 2.0-Diensten nach der US-amerikanischen Rechtslage herbeizuführen, würden zwei relativ geringfügige Maßnahmen ausreichen.[1347] Zum einen müsste sichergestellt werden, dass im Rahmen der Voraussetzung des unmittelbaren wirtschaftlichen Vorteils gemäß § 512(c)(1)(B) ausreichend berücksichtigt werden kann, dass im Einsatz einer Content-Identification-Technologie grundsätzlich eine rechtstreue Haltung des ISPs zum Ausdruck kommt. Ein ISP, der sich so verhält, sollte grundsätzlich auch dann von der Haftungsbeschränkung geschützt werden, wenn sein Geschäftsmodell auf einem werbefinanzierten Geschäftsmodell beruht, dessen Erfolg von der Höhe des Nutzeraufkommens abhängig ist. Weiterhin müsste im Rahmen des *threshold requirement* gemäß § 512(i)(1)(B) die Definition des Begriffs der STMs optimiert werden, so dass der Einsatz von Technologien, die den Schutz von Urheberrechten objektiv verbessern, automatisch zur Voraussetzung der Anwendbarkeit der Haftungsbeschränkung wird und in seiner Entstehung nicht länger von der Willensbildung der durch die Entstehung von STMs betroffenen Interessengruppen abhängt.

Die Korrektur der Rechtslage nach deutsch-europäischem Recht wäre hingegen erheblich aufwendiger, allein aus dem Grund, dass hierfür eine Reform der Haftungsbeschränkungen für ISPs auf EU-Ebene erforderlich wäre. Denn aufgrund der durch Art. 12-15 ECRL bewirkten Vollharmonisierung kann der deutsche Gesetzgeber Änderungen, durch die die Anwendbarkeit der Haftungsbeschränkungen an weitere Voraussetzungen geknüpft werden würde, nicht im Alleingang vornehmen. Es ist somit der europäische Gesetzgeber gefordert, im Zusammenhang mit den Haftungsbeschränkungen für ISPs einen Anreiz zum Einsatz von Technologien zu schaffen, durch die der Schutz von Urheberrechten maßgeblich verbessert wird. Insoweit käme insbesondere eine Klarstellung im Text der Regelungen der Richtlinie in Ergänzung zu Erwägungsgrund 42 in Betracht. Demnach sollten ISPs den Schutz einer Haftungsbeschränkung grundsätzlich nur beanspruchen können, wenn ihnen die Kontrolle des in Frage stehenden rechtswidrigen Verhaltens der Nutzer trotz des Einsatzes verfügbarer Technologien nicht möglich ist.

1347 Vgl. 8. Kapitel, Teil B.IV.3.a.cc.

Teil 4:
Zusammenfassung und Fazit

"Copyright, as embodied in the Statute of Anne and in our copyright acts, has not been concerned with the ability to express thoughts, but instead with protecting the author's way of expressing those thoughts. Neither did copyright arise in reaction of the (much earlier) introduction of the printing press…"[1348]

9. Kapitel: Zusammenfassung der Ergebnisse bezüglich des Einsatzes von DRM-Systemen im Multimediabereich

Die Digitalisierung in Kombination mit der zunehmenden, weltweiten Verbreitung breitbandiger Internetverbindungen, die zu einer unbeschränkten Vervielfältigungs- und Verbreitungsmöglichkeit von digitalen Multimediawerken führt, hat einen tiefgreifenden Wandel in der Multimediaindustrie ausgelöst. Denn die neuen technischen Parameter haben erhebliche Auswirkungen auf die ökonomischen Grundregeln, denen dieser Industriezweig bisher gefolgt ist.

An der Entwicklung der Musikindustrie der letzten zehn Jahre zeigen sich deutlich sowohl die Symptome der Krise, der sich die Multimediaindustrie derzeit aufgrund der Digitalisierung ausgesetzt sieht, als auch mögliche Auswege aus dem digitalen Dilemma. So ließ sich in dieser Branche zunächst die völlige Ablehnung der neuen Realität beobachten, Tonaufnahmen im Binärcode auf frei austauschbarem und unbegrenzt zur Verfügung stehendem Speicherplatz abspeichern und über das Internet verbreiten zu können. Auf die entsprechend veränderte Nachfrage der Nutzer reagierte die Musikindustrie nicht mit der Schaffung attraktiver legaler Möglichkeiten, digitale Inhalte schnell und einfach über das Internet zu erwerben. Vielmehr propagierte sie den weitestgehenden Einsatz von DRM-Systemen, mit deren Hilfe die hauptsächlichen Errungenschaften der Digitalisierung, nämlich die unbegrentzte Möglichkeit der Vervielfältigung und Verbreitung digitaler Inhalte, wieder rückgängig gemacht werden sollten, um hierdurch die Kontrolle über die Vertriebswege wiederzuerlangen. Auf diese Weise sollte das tradierte Geschäftsmodell vor allem der Tonträgerunternehmen in die Ära der Digitalisierung hinübergerettet werden, das fast vollständig von dem Vertrieb von Tonaufnahmen über physische Datenträger und damit von den pro abgesetzten Datenträger erzielten

1348 *Patry*, in: Patry on Copyright, 2010, § 8:2, 8-7.

Einnahmen abhing. Mit Hilfe internationaler Verträge und der nationalen Gesetzgeber wurde der Einsatz von DRM-Systemen entgegen den Interessen der Nutzer auch auf rechtlicher Ebene abgesichert und der Einsatz technischer Schutzmaßnahmen sowie deren rechtlicher Schutz weitgehend zum Selbstzweck erhoben, unabhängig davon, ob dies dem urheberrechtlich vorgesehenen Interessenausgleich zwischen den Interessen der Rechtsinhaber und der Nutzer dient. Denn die insoweit eingeführten gesetzlichen Umgehungsverbote bezogen auch soche Handlungen in ihren Tatbestand ein, deren Zweck aufgrund der Fair-Use-Doktrin bzw. der urheberrechtlichen Schrankenbestimmungen in gewissem Umfang urheberrechtlich legitimiert ist.

Dennoch scheiterte der Einsatz von DRM-Systemen in dem für die Musikindustrie so wichtigen Marktsegment der digitalen Downloads. Denn diese Systeme waren Teil eines Geschäftsmodells, das grundsätzliche Aspekte der Nutzerfreundlichkeit vernachlässigte. So wurde der Wunsch der Nutzer nach Interoperabilität zwischen digitalen Inhalten und digitalen Endgeräten sowie die berechtigte Erwartung der Wahrung sonstiger Rechtsgüter, insbesondere der Unversehrtheit des Eigentums und des Rechts auf informationelle Selbstbestimmung, durch den Einsatz von DRM-Systemen beim Vertrieb von Musikdownloads missachtet. Dies führte innerhalb kurzer Zeit dazu, dass die Nutzer die ihnen von der Multimediaindustrie zum legalen Konsum digitaler Inhalte angebotenen, auf DRM-Systemen basierenden Geschäftsmodelle ablehnten. Diese Ablehnung wurde durch die zusätzliche rechtliche Absicherung, die DRM-Systeme in Form der Umgehungsverbote genossen, noch zusätzlich bestärkt. Denn es entstand der Eindruck, dass im Hinblick auf den Vertrieb von digitalen Inhalten zugunsten der Rechtsinhaber ein besonderes *Paracopyright* geschaffen wurde, das zum Nachteil der Nutzer von urheberrechtlich geschützten Werken von dem „normalen" Urheberrecht abwich, indem den Nutzern die Ausübung auch bislang urheberrechtlich legitimierter Nutzungshandlungen unmöglich gemacht wurde. Diese Vernachlässigung ihrer legitimen Interssen beantworteten die Nutzer jedoch mit der Abwanderung in das *darknet*, d.h. in illegale Angebote, denen die Multimediaindustrie bisher nicht beizukommen vermochte und die, wie gezeigt wurde, aufgrund der immer fortschreitenden Verbreitung von Computern und Internet sowie des Phänomens des *analog hole* auch in Zukunft fortbestehen werden.

Nunmehr hat die Musikindustrie eingesehen, dass sie das von ihr präferierte Geschäftsmodell nicht gegen den Willen der Nutzer durchsetzen kann, solange diese die Möglichkeit haben, für sie unbefriedigende Angebote der Multimediaindustrie mit der Abwanderung in illegale Angebote zu beantworten. Sie hat sich daher zum einen vom DRM-gestützen Vertrieb von Musikdownloads weitgehend verabschiedet und sich zum anderen einer Reihe völlig neuer Geschäftsfelder, wie z.B. Abonnementmodellen, Live-Aufführungen und Merchandising zugewendet,

von denen sie sich Wachstumspotential verspricht. Eine wichtige Rolle nimmt hierbei die Kooperation mit Web 2.0-Diensten ein, in deren Rahmen die Lizenzgebühren, die für die Nutzung urheberrechtlich geschützter Inhalte auf diesen Internetdiensten zu entrichten sind, über die Zuschaltung von Werbebotschaften generiert werden. Ein Paradigmenwechsel ist in dieser Kehrtwende der Musikindustrie deswegen zu sehen, da der Fokus ihrer wirtschaftlichen Aktivität sich hierdurch mehr und mehr weg von dem Vertrieb einzelner Vervielfältigungsstücke einer Tonaufnahme (in Form physischer Datenträger) an die Nutzer verlagert, hin zu der Kommerzialisierung eines Inhalts mittels dessen Verbreitung über möglichst viele unterschiedliche Plattformen, wodurch eine möglichst große Anzahl von Nutzern auf den Inhalt aufmerksam werden und die in diesem Zusammenhang angebotenen Leistungen (Werbebotschaften, Merchandisingprodukte, Besuch von Live-Konzerten) in Anspruch nehmen soll. In diesem Zusammenhang spielt der Schutz eines Werks vor unberechtigtem Zugang durch technische Schutzmaßnahmen nicht nur keine Rolle mehr, sondern würde dem Ziel einer möglichst weitgehenden Verbreitung des Inhalts diametral entgegenlaufen.

Im Rückblick zeigt sich somit, dass die gesetzlichen Umgehungsverbote in Bezug auf technische Schutzmaßnahme ein Instrument zur Bewahrung eines Geschäftsmodells darstellten, bezüglich dessen sich herausgestellt hat, dass es sich im Zeitalter der Digitalisierung überholt hat und zumindest in wesentlichen Teilen durch neue, erst durch die Digitalisierung möglich gewordene Geschäftsmodelle ersetzt wird. Damit stellt sich jedoch immer drängender die Frage, ob angesichts dieser veränderten Umstände der rechtliche Umgehungsschutz noch eine Existenzberechtigung für sich beanspruchen kann. Diese Frage muss auch gestellt werden, da, wie gezeigt wurde, die Umgehungsverbote dazu beigetragen haben, ein Paracopyright zu schaffen, das in wesentlichen Aspekten zum Nachteil der Nutzer vom „normalen" Urheberrecht abweicht. Da das hinter den Umgehungsverboten stehende ökonomische Ziel der Rückgewinnung der Kontrolle über die Vertriebswege nicht erreicht werden kann, dürfte diese Frage zu verneinen sein. Denn die hehre Aufgabe des Urheberrechts besteht nicht darin, bestimmte Mittel und Wege, über die urheberrechtlich geschützte Werke für Dritte wahrnehmbar gemacht und an diese übermittelt werden können, zu schützen, sondern vielmehr eine persönliche geistige Schöpfung davor zu bewahren, dass in die mit ihr verbundenen Rechtspositionen eingegriffen wird.

10. Kapitel: Zusammenfassung der Ergebnisse bezüglich der Auswirkungen des Einsatzes von Content-Identification-Technologien auf die Haftung von Web 2.0-Diensten

Durch das Web 2.0 entsteht nunmehr ein weiteres Dilemma für die Rechtsinhaber: einerseits bieten Web 2.0-Dienste den Nutzern vielfältige Möglichkeiten, Urheberrechte zu verletzen. Andererseits stellen diese Dienste ein extrem effektives Marketing- und Verbreitungsinstrument dar, das es den Rechtsinhabern ermöglicht, die Aufmerksamkeit der breiten Öffentlichkeit auf ein urheberrechtlich geschütztes Multimediawerk zu lenken und hierdurch Kommerzialisierungsmöglichkeiten zu eröffnen. Insoweit bieten vor allem werbefinanzierte Geschäftsmodelle, auf denen vor allem soziale Netzwerke und Videoplattformen zumeist basieren, großes Wachstumspotential. Der technische Fortschritt im Bereich der Content-Identification-Technologien eröffnet zudem die Möglichkeit, urheberrechtlich geschützte Multimediawerke auf Web 2.0-Diensten zu identifizieren, zu löschen oder durch die automatische Zuschaltung von Werbung kommerziell fruchtbar zu machen. Durch diese ständig fortentwickelten und verbesserten Technologien wird es somit möglich, die Verbreitung und Verfügbarmachung von digitalen Multimediawerken im Internet besser zu kontrollieren und zu steuern.

Damit werden jedoch gleichzeitig die Haftungsbeschränkungen für Host-Provider und damit der zweite wichtige Bereich von Gesetzgebungsakten, die speziell angesichts der Herausforderungen des digitalen Zeitalters, insbesondere des Internets, in den USA und im deutsch-europäischen Rechtskreis geschaffen wurden, auf den Prüfstein gestellt. Die im Rahmen der vorliegenden Arbeit durchgeführte Analyse hat gezeigt, dass gesetzgeberische Maßnahmen, die als Antwort auf eine spezifische technische Neuentwicklung erfolgen, ein hohes Risiko laufen, daran zu scheitern, dass sie zukünftige Entwicklungen, durch die solche technischen Errungenschaften regelmäßig modifiziert und verändert werden, mangels juristischer Evolutionselastizitäten nicht adäquat berücksichtigen können. Die Haftungsbeschränkungen wurden vor dem Hintergrund eingeführt, dass man die Haftungsrisiken der ISPs für Rechtsverletzungen, die Nutzer innerhalb ihrer Dienste begehen, begrenzen wollte, weil sie diese Rechtsverletzungen einerseits nicht kontrollieren konnten und andererseits ihre Dienstleistungen als wichtig für die Fortentwicklung des Internets und des E-Commerce erachtet wurden. Allerdings sehen weder der US-amerikanische noch der deutsch-europäische Ansatz zur Beschränkung der Haftung von ISPs eine adäquate, effektive Reaktionsmöglichkeit für den Fall vor, dass den ISPs die Kontrolle des innerhalb ihrer Dienste abgewickelten Datenverkehrs und damit der Rechtsverletzungen der Nutzer nachträglich möglich wird.

In den USA läuft daher gegenwärtig ein ISP, der Content-Identification-Technologien einsetzt, Gefahr, deswegen den Schutz der Haftungsbeschränkung zu verlieren, da er damit die Kontrolle über rechtswidriges Nutzerverhalten erhält. Damit befindet er sich jedoch in einer schlechteren Position als sein Konkurrent, der keine solche Technologie einsetzt, und der wegen des Ausschlusses allgemeiner proaktiver Überwachungspflichten auch nicht dazu verpflichtet werden kann, eine solche Technologie einzusetzen. Eine solche Verpflichtung wäre einzig möglich, sofern die Technologie eine STM darstellt. Aufgrund der misslungenen Definition von STMs ist jedoch weitgehend sicher, dass diese niemals zur Entstehung gelangen werden. Dieses unbefriedigende Ergebnis wird lediglich durch das Notice&Takedown-Verfahren weitgehend entschärft, wodurch die eigentliche rechtliche Auseinandersetzung auf die Ebene des Rechtsinhabers und des Nutzer eingegrenzt wird, aber dafür dem Rechtsinhaber ein klar geregeltes und effektives Verfahren zur Verfügung gestellt wird, um Rechtsverletzungen zügig durch einen ISP beseitigen zu lassen.

Auch nach deutsch-europäischem Recht besteht keine Handhabe, um auf die veränderten Kontrollmöglichkeiten der ISPs adäquat zu reagieren. Zwar ist nach den Erwägungsgründen der E-Commerce-Richtlinie die Kontrolle der ISPs über rechtswidrige Inhalte der Hauptanknüpfungspunkt für dessen Haftung, jedoch findet diese grundlegende Annahme keinen Widerhall in den eigentlichen Regelungen der Haftungsbeschränkungen. Zudem sind auch nach deutsch-europäischem Recht proaktive Überwachungspflichten ausdrücklich ausgeschlossen, so dass auch aus diesem Grund die Verpflichtung des ISPs, Content-Identification-Technologien zum Schutz von Urheberrechten einzusetzen, ausscheidet. In Deutschland wird diese unbefriedigende Situation allein dadurch ausgeglichen, dass sich der BGH standhaft weigert, die Haftungsbeschränkungen auch auf die Störerhaftung anzuwenden und den gesetzlich ausdrücklich festgehaltenen Ausschluss allgemeiner Überwachungspflichten bei der Bestimmung des Umfangs der dem ISP obliegenden Prüfpflichten zu berücksichtigen. Auf diese Weise bleibt es – allerdings um den Preis des Verlusts der Rechtssicherheit betreffend die Voraussetzungen der Haftung von ISPs – möglich, Einzelfallabwägungen vorzunehmen, in deren Rahmen insbesondere auch die einem ISP tatsächlich zur Verfügung stehenden technischen Kontrollmöglichkeiten berücksichtigt werden können.

11. Kapitel: Fazit

„The answer to the machine is not in the machine." So lassen sich die Ergebnisse des ersten Schwerpunkts dieser Arbeit auf den Punkt bringen. Dies bedeutet, dass auch im Zeitalter der Digitalisierung den Marktteilnehmern auf dem Markt für Multimediawerke nicht erspart bleibt, sich auf die neuen Gegebenheiten des Marktes einzustellen und diese anzuerkennen. Denn die Entwicklung in der Musikindustrie ist ein eindrucksvoller Beleg dafür, dass es nicht möglich ist, die neuen Vervielfältigungs- und Verbreitungsmöglichkeiten durch technische Schutzmaßnahmen effektiv zu bekämpfen und zu eliminieren, sondern diese ein unabänderliches Faktum darstellen, an dem es nichts mehr zu Rütteln gibt. Auch der spezielle Schutz, den das internationale und nationale Recht solchen technischen Schutzmaßnahmen gewährt, vermag hieran nichts zu ändern. Es gilt somit, die „normative Kraft des Faktischen" anzuerkennen und die neuen Gegebenheiten als Chance für neue Geschäftsfelder und Wachstumspotentiale zu begreifen. Der Erfolg solcher zukünftiger Geschäftsmodelle wird davon abhängen, die neuen technischen Umstände und die dadurch veränderten Erwartungen der Nutzer mit den berechtigten Interessen der Rechtsinhaber an der wirtschaftlichen Nutzbarmachung ihrer Rechtspositionen in Einklang zu bringen. Dass dies kein Ding der Unmöglichkeit ist, zeigt sich wiederum an der Musikindustrie, deren Hinwendung zu neuen Geschäftsfeldern, wie z.B. den DRM-freien Vertrieb von Musikdownloads über viele verschiedene Anbieter, berechtigten Anlass zu der Hoffnung gibt, dass in diesem Industriezweig die Trendwende hin zu neuem Wachstum bald Realität werden wird.

Weiterhin zeigen die Ergebnisse des zweiten Schwerpunkts dieser Arbeit, dass eine Haftungsfreizeichnung von bestimmten Marktteilnehmern allein auf der Grundlage sich ständig fortentwickelnder und sich überholender technologischer Gegebenheiten wenig interessengerecht ist. Viel zu groß ist die Gefahr, dass kurze Zeit später die Gründe, die eine besondere Schutzwürdigkeit der privilegierten Marktteilnehmer ursprünglich zu rechtfertigen schienen, obsolet werden. Tritt dieser Fall ein, führt dies jedoch zu einem Ungleichgewicht der Interessen aller von der Haftungsbeschränkung Betroffenen, in diesem Fall derjenigen, deren Rechte verletzt werden, und die dann keine Möglichkeit haben, gegen diese Rechtsverletzungen durch Inanspruchnahme der ISPs effektiv vorzugehen. Das Ergebnis ist somit eine gleichsam „institutionalisierte" partielle Rechtlosstellung der Betroffenen. Wenn dennoch solche Haftungsbeschränkungen geschaffen werden sollen, gilt es darauf zu achten, in den entsprechenden gesetzlichen Regelungen den Schutzzweck und die speziellen Umstände, die die Haftungsbeschränkung im Zeitpunkt ihrer Schaffung zu rechtfertigen scheinen, festzuhalten. Auch muss sichergestellt werden, dass die Regelungen ausreichend darauf reagieren können, wenn

eine dieser Grundvoraussetzungen – und damit die Rechtfertigung für die Gewährung der haftungsrechtlichen Besserstellung – nachträglich entfällt.

Die vorliegende Arbeit hat gezeigt, dass es höchst riskant ist, neue technische Entwicklungen mit Hilfe des Rechts „einfangen" und in eine bestimmte Richtung steuern zu wollen. Denn es besteht die nicht zu unterschätzende Gefahr, dass rechtliche Regelungen der technischen Entwicklung im Ergebnis lediglich „hinterherrennen", diese Prozesse jedoch nicht wirklich im Sinne der Betroffenen, die sie schützen wollen, lenken können. Auch widerspricht dies dem Prinzip der Entwicklung eines technikneutralen Rechtssystems und insbesondere Urheberrechts.

Zudem verändern sich aufgrund des stetigen technischen Fortschritts die Grundlagen, aufgrund derer solche rechtliche Regelungen geschaffen werden, ständig. Neue Technologien stellen somit ein „moving target" dar, die den auf sie zugeschnittenen rechtlichen Regelungen ein gehöriges Maß an Dynamik abverlangen, damit diese sich nicht innerhalb kürzester Zeit überholen oder gar zu Ergebnissen führen, die ihrer eigentlichen Intention zuwiderlaufen. Es gilt somit, sich gerade bei der Schaffung von Regelungen im Zusammenhang mit neuen technischen Entwicklungen auf die rechtsimmanenten Grundsätze des Urheberschutzes zu besinnen. Denn nur wenn neben den Grundlagen, auf denen diese Regelungen basieren, auch die Ziele, die diese Regelungen im Rahmen des Urheberschutzes verfolgen, unmißverständlich zum Ausdruck kommen, ist für die Zukunft sichergestellt, dass diese Regelungen nur soweit und solange Anwendung finden werden, wie die tatsächlichen Parameter fortbestehen, auf deren Grundlage sie ursprünglich geschaffen wurden.

Literaturverzeichnis

Kommentare

Dreier, Thomas/Schulze, Gernot Urheberrechtsgesetz, 3. Auflage, München 2008 (zitiert als: *Autor*, in: *Dreier/Schulze*, UrhG, 2008)

Goldstein, Paul Copyright, 2. Auflage, New York, 2005 Supplement (zitiert als: *Goldstein*, Copyright, 2005)

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin (Hrsg.) Kommentar zur Europäischen Union, Band IV – Sekundärrecht, München, Stand Oktober 2009 (zitiert als: *Autor*, in: *Grabitz/Hilf/Nettesheim* (Hrsg.), EU, 2009)

Heckmann, Dirk Juris-Praxiskommentar Internetrecht (Telemediengesetz, E-Commerce, E-Government), Saarbrücken, 2007, (zitiert als: *Autor*, in: *Heckmann*, jurisPK-Internetrecht, 2007)

Löwenheim, Ulrich (Hrsg.) Handbuch des Urheberrechts, 2. Auflage, München 2010 (zitiert als: *Autor*, in: *Loewenheim* (Hrsg.), HdB UrhR, 2010)

Nimmer, Melville B./Nimmer, David Nimmer on Copyright, Band 3, Matthew Bender Revised Edition (Stand Dezember 2009) (zitiert als: *Nimmer*, in: Nimmer on Copyright, 2009)

Nordemann, Wilhelm/Nordemann, Axel/Nordemann, Jan Bernd (Hrsg.) Urheberrecht, 10. Auflage, Stuttgart 2008 (zitiert als: *Autor*, in: *Fromm/Nordemann* (Hrsg.), UrhR, 2008)

Patry, William F. Patry on Copyright, Volume 3, 2010 Thomson Reuters/West (zitiert als: *Autor*, in: *Patry* on Copyright, 2010)

Palandt, Otto Bürgerliches Gesetzbuch, 69. Auflage, München 2010 (zitiert als: *Autor*, in: *Palandt*, BGB, 2010)

Rebmann, Kurt/Säcker, Jürgen (Hrsg.) Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 5 (§§ 705-853), 4. Auflage, München 2004 (zitiert als: *Autor*, in: *Rebmann/Säcker* (Hrsg.), MüKo, BGB, 2004)

Schricker, Gerhard (Hrsg.) Urheberrecht, 3. Auflage, München 2006 (zitiert als: *Autor*, in: *Schricker* (Hrsg.), UrhR, 2006)

Spindler, Gerald/Schmitz, Peter/Geis, Ivo Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz, München 2004 (zitiert als: *Autor*, in: *Spindler/Schmitz/Geis*, TDG, 2004)

Monographien

Akester, Patricia Technological accommodation of conflicts between freedom of expression and DRM: the first empirical assessment, Cambridge, 2009, abrufbar unter: http://www.law.cam.ac.uk/faculty-resources/download/technological-accommodation-of-conflicts-between-freedom-of-expression-and-drm-the-first-empirical-assessment/6286/pdf (zitiert als: *Akester*, Technological Accommodation, 2009)

Bechtold, Stefan Vom Urheber- zum Informationsrecht – Implikationen des Digital Rights Management, München 2002 (zitiert als: *Bechtold*, DRM, 2002)

Becker, Eberhard/Buhse, Willms/Günnewig, Dirk/Rump, Niels (Hrsg.) Digital Rights Management – Technological, Economic, Legal and Political Aspects, Berlin Heidelberg 2003 (zitiert als: *Autor*, in: *Becker/Buhse/Günnewig/Rump* (Hrsg.), DRM, 2003)

Bernstein, Arthur/Sekine, Naoki/Weissman, Dick The Global Music Industry – Three Perspectives, New York/London 2007 (zitiert als: *Bernstein/Sekine/Weissman*, Global Music Industry, 2007)

Frahm, Christian Die Zukunft der Tonträgerindustrie, Boizenburg, 2007 (zitiert als: *Frahm*, Zukunft der Tonträgerindustrie, 2007)

Clement, Michel/Schusser, Oliver/Papies, Dominik (Hrsg.) Ökonomie der Musikindustrie, 2. Auflage, Wiesbaden 2008 (zitiert als *Autor*, in: *Clement/Schusser/Papies (Hrsg.)*, Ökonomie Musikindustrie, 2008)

Cooter, Robert/Ulen, Thomas Law & Economics, 5. Auflage, 2008 (zitiert als: *Cooter/Ulen*, Law & Economics, 2008)

Dustmann, Andreas Die privilegierten Provider – Haftungseinschränkungen im Internet aus urheberrechtlicher Sicht, Baden-Baden, 2001 (zitiert als: *Dustmann*, Privilegierte Provider, 2001)

Ernst, Stefan/Vassilaki, Irini/Wiebe, Andreas Hyperlinks – Rechtsschutz Haftung Gestaltung, Köln 2002 (zitiert als: *Autor*, in: *Ernst/Vassilaki/Wiebe*, Hyperlinks, 2002)

Ficsor, Mihaly The Law of Copyright and the Internet – The 1996 WIPO Treaties, their Interpretation and Implementation, New York 2002 (zitiert als: *Ficsor*, WIPO Treaties, 2002)

Fränkl, Gerald/Karpf, Philipp Digital Rights Management Systeme – Einführung, Technologien, Recht, Ökonomie und Marktanalyse, München 2004 (zitiert als: *Fränkl/Karpf*, DRMS, 2004)

Frenzel, Tobias Akzeptanz von Systemen der digitalen Distribution im E-Commerce der Musikwirtschaft, Berlin, 2003 (zitiert als: *Frenzel*, Akzeptanz im E-Commerce, 2003)

Freytag, Stefan M. Haftung im Netz, München 1999 (zitiert als: *Freytag*, Haftung im Netz, 1999)

Haring, Bruce MP3 – Die digitale Revolution in der Musikindustrie, Freiburg 2002 (zitiert als: *Haring*, MP3, 2002)

Hoeren, Thomas/Sieber, Ulrich (Hrsg.) Handbuch Multimediarecht, 24. Auflage, München 2010 (zitiert als: *Autor*, in: *Hoeren/Sieber* (Hrsg.), Multimediarecht, 2010)

Huster, Sibylla Die Gewinnhaftung bei Patent- und Urheberrechtsverletzungen nach deutschem und U.S.-amerikanischem Recht, Berlin, 2009 (zitiert als: *Huster*, Gewinnhaftung, 2009)

Kouretsidis, Takis Der digitale Musikmarkt, Hamburg, 2007 (zitiert als: *Kouretsidis*, Digitaler Musikmarkt, 2007)

Köhler, Markus/Arndt, Hans-Wolfgang/Fetzer, Thomas Recht des Internet, 6. Auflage, Heidelberg/München 2008(zitiert als: *Köhler/Arndt/Fetzer*, Recht des Internet, 2008)

Krasilovsky, M. William/Shemel, Sidney This Business of Music – The Definitive Guide to the Music Industry, 10. Auflage, New York 2007 (zitiert als: *Krasilovsky/Shemel*, Music Business, 2007)

Lehmann, Michael (Hrsg.) Electronic Business in Europa – Internationales, europäisches und deutsches Online-Recht, München 2002 (zitiert: *Autor*, in: *Lehmann* (Hrsg.), Electronic Business, 2002)

Lehmann, Michael/Meents, Jan Geert (Hrsg.) Handbuch des Fachanwalts Informationstechnologierecht, Köln 2008 (zitiert als: *Autor*, in: *Lehmann/Meents* (Hrsg.), FA IT-Recht, 2008)

Merges, Robert P. /Menell, Peter S./Lemley, Mark A. Intellectual Property in the New Technological Age, 3. Auflage, New York 2003 (zitiert als: *Merges/Menell/Lemley*, Intellectual Property, 2003)

Meschede, Thomas Der Schutz digitaler Musik- und Filmwerke vor privater Vervielfältigung nach den zwei Gesetzen zur Regelung des Urheberrechts in der Informationsgesellschaft, Frankfurt 2007 (zitiert als: *Meschede*, Schutz digitaler Musik- und Filmwerke, 2007)

Mittenzwei, Julius Informationen zur Rechtewahrnehmung im Urheberrecht – Der Schutz von Digital Rights Management-Systemen und digitale Wasserzeichen durch § 95 c UrhG, München/Ravensburg 2006 (zitiert als: *Mittenzwei*, Informationen zur Rechtewahrnehmung, 2006)

Moritz, Hans-Werner/Dreier, Thomas Rechts-Handbuch zum E-Commerce, 2. Auflage, Köln 2005 (zitiert als: *Autor*, in: *Moritz/Dreier* (Hrsg.), RHdB E-Commerce, 2005)

Pankoke, Stefan L. Von der Presse- zur Providerhaftung, München 2000 (zitiert als: *Pankoke*, Von der Presse- zur Providerhaftung, 2000).

Reinbothe, Jörg/von Lewinski, Silke The WIPO Treaties 1996 – The WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty – Commentary and Legal Analysis, London/Edingburgh 2002 (zitiert als: *Reinbothe/Lewinski*, WIPO Treaties, 2002)

Reinke, Daniel Neue Wertschöpfungsmöglichkeiten der Musikindustrie – Innovative Businessmodelle in Theorie und Praxis, Baden-Baden 2009 (zitiert als: *Reinke*, Wertschöpfungsmöglichkeiten Musikindustrie, 2009)

Ross, Terence P. Intellectual Property Law – Damages and Remedies, New York 2000 (zitiert als: *Ross*, IP Law, 2000)

Roßnagel, Alexander (Hrsg.) Digitale Rechteverwaltung – Eine gelungene Alllianz von Recht & Technik?, Baden-Baden 2009 (zitiert als: *Autor*, in: *Roßnagel (Hrsg.)*, Digitale Rechteverwaltung, 2009)

Roßnagel, Alexander/Banzhaf, Jürgen/Grimm, Rüdiger Datenschutz im Electronic Commerce: Technik – Recht - Praxis, Heidelberg 2003 (zitiert als: *Roßnagel/Banzhaf/Grimm*, Datenschutz im E-Commerce, 2003)

Schäfer, Hans-Bernd/Ott, Claus The Economic Analysis of Law, Cheltenham/Northampton 2004 (zitiert als: *Schäfer/Ott*, Economic Analysis of Law, 2004)

Sieber, Ulrich Verantwortlichkeit im Netz, München 1999 (zitiert als: *Sieber*, Verantwortlichkeit im Netz, 1999)

Stadler, Thomas Haftung für Informationen im Internet, 2. Auflage, Berlin 2005 (zitiert als: *Stadler*, Informationen im Internet, 2005)

Ünlü, Vural Content Protection – Economic Analysis and Techno-legal Implementation, München 2005 (zitiert als: *Ünlü*, Content Protection, 2005)

Wand, Peter Technische Schutzmaßnahmen und Urheberrecht – Vergleich des internationalen, europäischen, deutschen und US-amerikanischen Rechts, München 2001 (zitiert als: *Wand*, Technische Schutzmaßnahmen, 2001)

Volkmann, Christian Der Störer im Internet – Zur Verantwortlichkeit der Internet-Provider im allgemeinen Zivil-, Wettbewerbs-, Marken- und öffentlichen Recht, München, 2005 (zitiert als: *Volkmann*, Der Störer im Internet, 2005)

Aufsätze

Arlt, Christian Digital Rights Mangement Systeme. Begriff, Funktion und rechtliche Rahmenbedingungen nach den jüngsten Änderungen des UrhG – insbesondere zum Verhältnis der §§ 95 a ff. UrhG zum Zugangskontrolldiensteschutzgesetz, GRUR 2004, 548-554

Azim-Khan, Rafi/Farmer, Steven User Generated Content Provider finds Safe Harbor Following Allegations of Copyright Infringement, 2009 Ent. L. R. 20(2) 55-57

Band, Jonathan Anmerkung zum Urteil *Perfect 10 v. CCBill,* 488 F.3 d 1102 (9th Cir. 2007), CRi 2007, 122-124

Bayreuther, Frank Beschränkungen des Urheberrechts nach der neuen EU-Urheberrechtsrichtlinie, ZUM 2001, 829-839

Beckermann, Ray Content Holders vs. The Web: 2008 US Copyright Law Victories Point to Robust Internet, Journal of Internet Law 12/7 16-21 (2009)

Beaty, Tiffany N. Navigating the Safe Harbor Rule: The Need For a DMCA Compass, 13 Marq. Intell. Prop. L. Rev. 207-227 (2009)

Bender, Rolf/Kahlen, Christine Neues Telemediengesetz verbessert den Rechtsrahmen für Neue Dienste und Schutz vor Spam-Mails, MMR 2006, 590-594

Berger, Arndt/Janal, Ruth Suchet und Ihr werdet finden? Eine Untersuchung zur Störerhaftung von Online-Auktionshäusern, CR 2004, 917-925

Biddle, Peter/England, Paul/Peinado, Marcus/Willman, Bryan The Darknet and the Future of Content Distribution, abrufbar unter http://msl1.mit.edu/ESD10/docs/darknet5.pdf

Braverman, Alan N./Southwick, Terri The User-Generated Content Principles: The Motiviation, Process, Results and Lessons Learned, 32 Colum. J.L. & Arts 471-480 (2009)

Bretan, Jennifer Harboring Doubts About the Efficacy of § 512 Immunity Under the DMCA, 18 Berkeley Tech L.J. 43-67 (2003)

Christiansen, Peer Anmerkung zum Urteil des LG Köln vom 26.11.2003 (28 O 706/02), MMR 2004, 185-186

Clark, Charles The Answer to the Machine is in the Machine, in: *Hugenholtz* (Hrsg.), The Future of Copyright in a Digital Environment, The Hague 1996, S. 139-148

Czychowski, Christian Das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft – Ein Über- und Ausblick, NJW 2003, 2409-2412

Darrow, Jonathan J./Ferrera, Gerald R. Social Networking Web Sites and the DMCA: A Safe-Harbor from Copyright Infringement Liability or the Perfect Storm?, 6 Nw. J. Tech. & Intell. Prop. 1-35 (2007)

Dimitrieva, Irina Y. I Know It When I See It: Should Internet Providers Recognize Copyright Violation When They See It?, 16 Santa Clara Computer & High Tech. L.J. 233-261 (2000)

Dreier, Thomas Die Umsetzung der Urheberrechtsrichtlinie 2001/29/EG in deutsches Recht, ZUM 2002, 28-43

Dreyer, Gunda Urheberrechtliche Problembereiche des Digital Rights Management, in: *Louis Pahlow/Jens Eisfeld* (Hrsg.), Grundlagen und Grundfragen des Geistigen Eigentums, Tübingen 2008, S. 221-250

Driscoll, Michael Will YouTube Sail into the DMCA's Safe Harbor or Sink for Internet Piracy?, 6 J. Marshall Rev. Intell. Prop. L. 550-569 (2007)

Eck, Stefan/Ruess, Peter Haftungsprivilegierung der Provider nach der E-Commerce-Richtlinie. Umstzungsprobleme dargestellt am Beispiel der Kenntnis nach § 11 Satz 1 Ziff. 1 TDG, MMR 2003, 363-366

Einhorn, Michael A. Thinking Outside the Box: The Next Generation Moves in the Music Business, 56 J. Copyright Soc'y, 201-211 (2008)

ders. Gorillas in Our Midst: Searching for King Kong in the Music Jungle, 2007, abrufbar unter http://ssrn.com/abstract=1030886
(zitiert als: Einhorn, Gorillas in Our Midst, 2007)

Engels, Stefan Zivilrechtliche Haftung für Inhalte im World Wide Web, AfP 2000, 524-529

Engel-Flechsig, Stefan/Maennel, Frithjof/Tettenborn, Alexander Das neue Informations- und Kommunkationsdienste-Gesetz, NJW 1997, 2981-2992

Fitzner, Julia Fortbestehende Rechtsunsicherheit bei der Haftung von Host-Providern - Anwendbarkeit der Haftungsbeschränkung nach TMG und der aktuellen Rechtsprechung, MMR 2011, 83-86

Flechsig, Norbert P. Digitales Rechtemanagement im Lichte ergänzender Schutzbestimmungen – Inhalt und Bedeutung des Digital Rights Mangement aus urheberrechtlicher Sicht – oder Technik vor Recht?, in: *Loewenheim, Ulrich* (Hrsg.), Urheberrecht im Informationszeitalter, Festschrift für Wilhelm Nordemann, München 2004, S. 313-320

Fülbier, Ulrich Web 2.0 – Haftungsbeschränkungen bei MySpace und YouTube, CR 2007, 515-521

Freytag, Stefan Digital Millennium Copyright Act und europäisches Urheberrecht für die Informationsgesellschaft, MMR 1999, 207-213

ders. Providerhaftung im Binnenmarkt. Verantwortlichkeit für rechtswidrige Inhalte nach der E-Commerce-Richtlinie, CR 2000, 600-609

Gerke, Marco Verantwortlichkeit des Betreibers eines Meinungsforums, MMR 2003, 602-603

Ginsburg, Jane C. Separating the Sony Sheep From the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs, 50 Ariz. L. Rev. 577, 578-609 (2008)

dies. The (new?) Right of Making Available to the Public, 2004, abrufbar unter http://ssrn.com/abstract=602623

Hilty, Reto M. Rechtsschutz technischer Maßnahmen: Zum UrhG-Regierungsentwurf vom 31.7.2002, MMR 2002, 577-578

Holznagel, Bernd/Brüggemann, Sandra Das Digital Right Management nach dem ersten Korb der Urheberrechtsnovelle – Eine verfassungsrechtliche Beurteilung der neuen Kopierschutzregelungen, MMR 2003, 767ff.

Holznagel, Daniel Zur Providerhaftung Notice and Take-Down in § 512 U.S. Copyright Act, GRUR Int 2007, 971-986

Hoeren, Thomas Entwurf einer EU-Richtlinie zum Urheberrecht in der Informationsgesellschaft - Überlegungen zum Zwischenstand der Diskussion, MMR 2000, 515-521

Hoeren, Thomas Anmerkung zu BGH, BGH, Urteil v. 11. 3. 2004, I ZR 304/01 – Internetversteigerung, MMR 2004, 672-673

ders. Das Telemediengesetz, NJW 2007, 801-806

Hughes, Justin On the Logic of Suing One's Customers and the Dilemma of Infringement-Based Business Models, 22 Cardozo Arts & Ent. L.J. 725-766 (2005)

Ingendaay, Dominik Künstlerverträge in Deutschland und den USA, DAJV Newsletter 2009, 108-114

Jürgens, Uwe/Veigel, Ricarda Zur haftungsminimierenden Gestaltung von „User Generated Content"-Angeboten, AfP 2007, 181-187

Katyal, Sonia K. Filtering, Piracy Surveillance and Disobedience, 32 Colum. J.L. & Arts, 401-426 (2009)

Kim, Eugene C. YouTube: Testing the Safe Harbors of Digital Copyright Law, 17 S. Cal. Interdis. L.J. 139-171 (2007)

Klatt, Heiko Die Kerngleichheit als Grenze der Prüfungspflichten und der Haftung des Hostproviders, ZUM 2009, 265-275

Kröger, Detlef Die Urheberrechtsrichtlinie für die Informationsgesellschaft – Bestandsaufnahme und kritische Bewertung, CR 2001, 316-324

Lauber, Anne/Schwipps, Carsten Das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, GRUR 2004, 293-300

Lee, Edward Warming Up to User-Generated Content, 2008 U. Ill. L. Rev. 1459-1548 (2008)

Lehmann, Michael Unvereinbarkeit des § 5 Teledienstegesetz mit Völkerrecht und Europarecht, CR 1998, 232-234

ders. Rechtsgeschäfte und Verantwortlichkeit im Netz – Der Richtlinienvorschlag der EU-Kommission, ZUM 1999, 180-183

ders. Die IT-relevante Umsetzung der Richtlinie Urheberrecht in der Informationsgesellschaft, CR 2003, 553-557

ders. The Answer to the Machine is Not in the Machine, in: *Beier, Dietrich/Brüning-Petit, Laurence/Heath, Christopher* (Hrsg.), Festschrift für *Jochen Pagenberg*, Köln 2006, S. 413-419

Lehment, Cornelis Zur Störerhaftung von Online-Auktionshäusern, zugleich Anmerkung zum Urteil des Landgerichts Düsseldorf vom 29.10.2002 – 4 a O 464/01 – eBay, WRP 2003, 1058-1065

ders. Zur Haftung von Internet- Auktionshäusern – Anmerkung zum Urteil des BGH Internet-Versteigerung, GRUR 2005, 210-214

Leible, Stefan/Sosnitza, Olaf Haftung von Internetauktionshäusern – reloaded, NJW 2007, 3324-3326

Lemley, Mark A./Reese, R. Anthony Reducing Digital Copyright Infringement Without. Restricting Innovation, 56 Stan. L. Rev. 1345-1434(2004)

von Lewinski, Silke/Gaster, Jens L. Die Diplomatische Konferenz der WIPO 1996 zum Urheberrecht und zu Verwandten Schutzrechten – Ergebnisse und Folgen, ZUM 1997, 607-625

Lincoff, Bennett Common Sense, Accommodation and Sound Policy for the Digital Music Marketplace, 2 J. Int'l Media & Ent. L. 1-64 (2008-2009).

Manekshaw, Cyrus Sarosh Jan Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, 10 Comp. L. Rev. & Tech. J. 101-133 (2005)

Martin, Ali Digital Rights Management (DRM) in Online Music Stores: DRM-Encumbered Music Downloads' Inevitable Demise as a Result of the Negative Effects of Heavy-Handed Copyright Law, 28 Loy. L.A. Ent. L. Rev. 265, 266-294 (2008)

Meisel, John B. Economic and Legal Issues Facing YouTube and Similar Internet Hosting Web Sites, Journal of Internet Law 12/8 1, 8-16 (2009)

Meyers, Brette G. Filtering Systems or Fair Use? A Comparative Analysis of Proposed Regulations for User Generated Content, 26 Cardozo Arts & Entertainment L. J. 935-956 (2009)

Montagnani, Maria Lillà A New Interface Between Copyright Law and Technology: How User-Generated Content Will Shape The Future of Online Distribution, 26 Cardozo Arts & Ent. L.J. 719-773 (2009)

Mulligan, Deirdre K./Perzanowski, Aaron The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident, 22 Berkeley Tech. L. J. 1157-1232 (2007)

Nimmer, David Back From the Future: A Proleptic Review of the Digital Millennium Copyright Act, 16 Berkeley Tech. L.J. 855-876 (2001)

Nordemann, Jan Bernd Störerhaftung für Urheberrechtsverletzungen – Welche konkreten Prüfpflichten haben Hostprovider (Contentprovider)?, CR 2010, 653-661

Ott, Stephan Die Haftung von YouTube für urheberrechtsverletzende Uploads seiner Nutzer nach US-amerikanischem Recht, GRUR Int. 2008, 563-569

Perritt, Henry H. Jr. Music Markets and Mythologies, abrufbar unter http://www.kentlaw.edu/perritt/courses/property/perritt-music-market-myths-jan07.htm (zitiert als: Perritt, Music Markets and Mythologies)

ders. Flanking the DRM Maginot Line Against New Music Markets, 16 Mich. St. J. Int'l Law 113-151 (2007).

Reichman, Jerome H./Dinwoodie, Graeme/Samuelson, Pamela A Reverse Notice and Takedown Regime to Enable Fair Uses of Technically Protected Copyrighted Works, 22 Berkeley Tech. L.J. 981-1060 (2007)

Reinbothe, Jörg Die Umsetzung der EU-Urheberrechtsrichtlinie in deutsches Recht, ZUM 2002, 43-52

Reese, Todd E. Wading Through the Muddy Waters: The Court's Misapplication of Section 512(c) of the Digital Millennium Copyright Act, 34 Sw. U. L. Rev, 287-323 (2004)

Reese, R. Anthony The Relationship Between the ISP Safe Harbors and the Ordinary Rules of Copyright Liability, 32 Colum. J.L. & Arts 427-443 (2009)

Rohleder, Bernhard DRM – Herausforderung und Chance in der digitalen Welt, ZUM 2004, 203-204

Rosch, J. Thomas A Different Perspective on DRM, Symposium: Copyright, Digital Rights Management Technology, and Consumer Protection, 22 Berkeley Tech. L.J. 971-980 (2007).

Roßnagel, Alexander Das Telemediengesetz, NVwZ 2007, 743-748

von Rosenberg, Oliver Liability of Internet providers in the freamwork of the U.S. Digital Millennium Copyright Act, K&R 1999, 399-412

Rössl, Markus/Rössl,Martina Filterpflichten des Providers – Drittschutz durch Technik, CR 2005, 809-814

Roth, Monika Entering the DRM-free Zone: An Intellectual Property and Antitrust Analysis of the Online Music Industry, 18 Fordham Intell. Prop. Media & Ent. L.J. 515-540 (2008)

Rücker, Daniel Notice and take down-Verfahren für die deutsche Providerhaftung? – Zur Begrenzung der Unterlassungshaftung von Online-Diensten durch das „Verbot allgemeiner Überwachungspflichten", CR 2005, 347-355

Samuelson, Pamela Intellectual Property and the Digital Economy: why the Anti-Circumvention Regulations Need To Be Revised, 14 Berkeley Tech. L. J. 519-566 (1999)

Samuelson, Pamela/Schultz, Jason Should Copyright Owners Have to Give Notice About Their Use of Technical Protection Measures?, 6 J. Telecom. & High Tech. L. 41-75 (2007)

Schaar, Peter Datenschutz und Internet – Die Grundlagen, München 2002 (zitiert als: *Schaar*, Datenschutz und Internet, 2002)

Schack, Haimo Urheberrechtliche Schranken, übergesetzlicher Notstand und verfassungskonforme Auslegung, in: *Ohly, Ansgar* (Hrsg.), Perspektiven des geistigen Eigentums und Wettbewerbsrecht, Festschrift für Gerhard Schricker, 2005, S. 511-521

ders. Urheberrechtliche Gestaltung von Webseiten unter Einsatz von Links und Frames, MMR 2001, 9-17

Schippan, Martin Urheberrecht goes digital – Das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, ZUM 2003, 378-390

Schultz, Mark F. Live Performance, Copyright, and the Future of the Music Business, 43 U. Rich. L. Rev. 685-764 (2009)

Schulz, Daniela Der Bedeutungswandel des Urheberrechts durch Digital Rights Management – Paradigmenwechsel im deutschen Urheberrecht?, GRUR 2006, 470-477

Seidenberg, Steven Copyright in the Age of YouTube – As User-Generated Sites Flourish, Copyright Law Struggles to Keep Up, ABA Journal, February 2009, S. 47-51

Sessinghaus, Karel BGH-„Internet-Versteigerung" – ein gemeinschaftsrechtswidriges Ablenkungsmanöver?,WRP 2005, 697-703

Sieber, Ulrich Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (I) – Zur Umsetzung von § 5 TDG am Beispiel der Newsgroups im Internet, CR 1997, 581-598

Sharp, Nicola/Arewa, Olufunmilayo Is Apple Playing Fair? Navigating the iPod Fairplay DRM Controversy, 5 Nw. J. Tech. & Intell. Prop. 332 (2007)

Sloane, Peter S./McMahon, Sean P. Reviewing U.S. Copyright Law and the Internet in 2008, CRi 2009, 6-9

Sobola, Sabine/Kohl, Kathrin Haftung von Providern für fremde Inhalte. Haftungsprivilegierung nach § 11 TDG – Grundsatzanalyse und Tendenzen der Rechtsprechung, CR 2005, 443-450

Spindler, Gerald E-Commerce in Europa. Die E-Commerce-Richtlinie in ihrer endgültigen Fassung, MMR-Beilage 7/2000, 4-21

ders. Die zivilrechtliche Verantwortlichkeit von Internetauktionshäusern. Haftung für automatisch registrierte und publizierte Inhalte?, MMR 2001, 737-743

ders. Das Gesetz zum elektronischen Geschäftsverkehr – Verantwortlichkeit der Dienstean-bieter und Herkunftslandprinzip, NJW 2002, 921-927

ders. Europäisches Urheberrecht in der Informationsgesellschaft, GRUR 2002, 105-120

ders. Anmerkung zu BGH, Urteil v. 11. 3. 2004, I ZR 304/01 – Internetversteigerung, JZ 2005, 37-40

ders. Das neue Telemediengesetz – Konvergenz in sachten Schritten, CR 2007, 239-245

ders. Anmerkung zum Urteil des BGH vom 19.4.2007 – I ZR 35/04 – Internet-Versteigerung II, MMR 2007, 511-514

ders. Präzisierungen der Störerhaftung im Internet – Besprechung des BGH-Urteils „Kinderhochstühle im Internet", GRUR 2011, 101-108

Spindler, Gerald/Volkmann, Christian Die zivilrechtliche Störerhaftung der Internet-Provider, WRP 2003, 1-15

Tettenborn, Alexander/Bender, Gunnar/Lübben, Natalie/Karenfort, Jörg Rechtsrahmen für den elektronischen Geschäftsverkehr. Kommentierung zur EG-Richtlinie über den elektronischen Geschäftsverkehr und zum Elektronischen Geschäftsverkehr-Gesetz – EGG: Inhalt – Auswirkungen- Umsetzung in Deutschland, BB-Beilage 10/2001, 1-40

Vassilaki, Irini Strafrechtliche Haftung nach §§ 8 ff. TMG, MMR 2002, 659-661

Vinje, Thomas C. A Brave New World of Technical Protection Systems: Will There Still Be Room For Copyright?, EIPR 1996, 431-440

Volkmann, Christian Die Unterlassungsvollstreckung gegen Störer aus dem Online-Bereich. Zur Durchsetzung von Unterlassungstiteln nach § 890 ZPO und dem Verbot von Überwachungspflichten nach §§ 8 Abs. 2 S. 1 TDG/§ 6 Abs. 2 S. 1 MDStV, CR 2003, 440-447

ders. Anmerkung zu BGH, Urteil vom 27.3.2007 – VI ZR 101/06, K&R 2007, 398-400

ders. Aktuelle Entwicklungen in der Providerhaftung im Jahr 2008, K&R 2009, 361-363

Wimmers, Jörg/Heymann, Britta Wer stört? – Zur Haftung der Internetprovider für fremde Inhalte. Anmerkung zu den BGH- Entscheidungen *Internet-Versteigerung II* und *Jugendgefährdende Medien bei eBay*, MR-Int 2007, 222-226

Wu, Tim The Copyright Paradox, 2005 Sup. Ct. Rev. 229-255 (2005)

Zarins, Emily Notice Versus Knowledge Under the Digital Millennium Copyright Act's Safe Harbors, 92 Calif. L. Rev. 257-298 (2004)

Gesetze und Gesetzesmaterialien

International

WIPO Copyright Treaty, Treaty Doc. No. 105-17, S. 1 (1997)/36 I.L.M. 65

WIPO Performances and Phonograms Treaty, S. Treaty Doc. No. 105-17, S. 18 (1997)/36 I.L.M. 76

Revidierte Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst vom 9. September 1886, zuletzt geändert am 28. September 1979

Agreement on Trade-Related Aspects of Intellectual Property Rights BGBl 1994 II S. 1730

USA

Copyright Act of 1790, 1 Stat. 124 (1790)

Copyright Act of 1976, Pub. L. No. 94-553, 90 Stat. 2541

House of Representatives Report No. 105-551, Part 1, 105th Cong., 2 d Sess. (1998) (zitiert als: H.R. Rep. 105-551 (I))

House of Representatives Report No. 105-551, Part 2, 105th Cong., 2 d Sess. (1998) (zitiert als: H.R. Rep. 105-551 (II))

Senate Report No. 105-190, 105th Cong., 2 d Sess. (1998) (zitiert als: S. Rep. 105-190)

Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (Oktober 28, 1998)

Europäische Union

Grünbuch der Europäischen Kommission zum Urheberrecht und zu den verwandten Schutzrechten in der Informationsgesellschaft vom 19. 07.1995, KOM(95) 382 endg.

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt vom 18.11.1998, KOM(1998) 586 endg., ABl. Nr. C 30 vom 05.02.1999, S. 4

Geänderter Vorschlag der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt vom 17.08.1999, KOM(1999) 427 endg.

Änderungsvorschläge des Europäischen Parlaments zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt, Abl. EG Nr. C 279 vom 1.10. 1999, S. 389

Gemeinsamer Standpunkt(EG) Nr. 22/2000 vom 28.2.2000 im Hinblick auf den Erlaß einer Richtlinie des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt, ABl. Nr. C 128, S. 32

Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt vom 08.06.2000, ABl. EG Nr. L 178 vom 17.07.2000, S. 1

Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22.5.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABlEG Nr. L 167 vom 22.06.2001, S. 10

Erster Bericht der Kommission über die Anwendung der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 08.06.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, KOM(2003) 702 endg.

Bericht über die Anwendung der Richtlinie über die Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (2001/29/EG) vom 30.11.2007, SEC(2007) 1556, abrufbar unter http://ec.Europa.eu/internal_market/copyright/ copyright-infso/copyright-infso_en.htm

Grünbuch Urheberrechte in der wissensbestimmten Wirtschaft vom 16.7.2008, KOM(2008) 466 endg.

Einigung über EU-Telekom-Reform ebnet den Weg für Stärkung der Verbraucherrechte, ein offenes Internet, einen Telekom-Binnenmarkt und schnelle Internetanschlüsse für alle Bürger, MEMO/09/491 vom 5.11.2009, abrufbar unter http://Europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/491&format=HTML&aged=0&language=DE&gui Language=en

Deutschland

Urheberrechtsgesetz vom 09.09.1965, BGBl. I S. 1273, zuletzt geändert durch Artikel 83 des Gesetzes vom 17.12.2008, BGBl. I S. 2586

Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste Gesetz vom 13.06.1997, BGBl I 1997, S. 1870

Entwurf eines Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz – EGG) vom 17.05.2001, BT-Drs. 14/6098

Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr vom 14.12.2001, BGBl I 2001, S. 3721

Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft vom 16. August 2002, BGBl I S. 1774

Entwurf eines Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz – ElGVG) vom 23.10.2006, BT-Drs. 16/3078

Gesetz zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste vom 26.02.2007, BGBl 2007 I, S. 179

Zweites Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft vom 26.10.2007, BGBl I 2007 S. 2513

Gesetz zur Verbesserung der Durchsetzung von Rechte des geistigen Eigentums vom 7.7.2008, BGBl. I S. 1191

Sonstige Materialien

Berkman Center for Internet and Society at Harvard Law School iTunes: How Copyright, Contract, and Technology Shape the Business of Digital Media – a Case Study, 2004, abrufbar unter http://cyber.law.harvard.edu/media/uploads/81/iTunesWhitePaper0604.pdf

Bundesjustizministerium „Berliner Rede zum Urheberrecht", Rede der Justizministerin Sabine Leutheusser-Schnarrenberger vom 14.06.2010, abrufbar unter http://www.bmj.bund.de/enid/0,41c20c636f6e5f6964092d093639339093a095f7472636964092d0936393230/Reden/Sabine_Leutheusser-Schnarrenberger_1mt.html

Bundesverband der Musikindustrie ("BVMI") Deutsche Musikindustrie begrüßt geplante Vereinbarung mit US-Providern zur Bekämpfung von Internetpiraterie, 19.12.2008, abrufbar unter http://www.musikindustrie.de/presse_aktuell_einzel/back/82/page5/news/deutsche-musik industrie-begruesst-geplante-vereinbarung-mit-us-providern-zur-bekaempfung-von-internetpi/

BVMI GFK Musikmarktprognose 2009, 17.09.2009, abrufbar unter http://www.musikindustrie. de/fileadmin/news/presse/090917_Musikmarktprognose_FINAL_dk.pdf

BVMI Homepage, Abteilung Recht-Privatkopien-Kopierschutz, abrufbar unter http://www.musikindustrie.de/kopierschutz/

Center for Democracy & Technology ("CDT") Evaluating DRM: Building a Marketplace for the Convergent World, Version 1.0, September 2006, abrufbar unter http://www.cdt.org/copyright/20060907drm.pdf
(zitiert als: *CDT*, Evaluating DRM, 2006)

Electronic Frontier Foundation ("EFF") RIAA v. The People: Five Years Later, abrufbar unter: http://www.eff.org/wp/riaa-v-people-years-later
(zitiert als: *EFF*, RIAA v. The People)

Fraunhofer Institut für Digitale Medientechnologie (IDMT)/Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)/Institut für Medien- und Kommunikationswissenschaft der TU Ilmenau (IfMK) „privacy4DRM" – Datenschutzverträgliches und nutzungsfreundliches Digital Rights Management, Studie im Auftrag des Bundesministeriums für Bildung und Forschung, Ilmenau/Kiel 2005, abrufbar unter https://www.datenschutzzentrum.de/drm/privacy4drm.pdf

INDICARE ("INformed DIalogue about Consumer Acceptability of DRM Solutions in Europe") Digital Rights Management and Consumer Acceptability, 2005, abrufbar unter http://www.indicare.org/tiki-download_file.php?fileId=111

International Federation of the Phonographic Industry ("IFPI") Recorded Music Sales 2008, abrufbar unter http://www.ifpi.org/content/library/Recorded-Music-Sales-2008.pdf
(zitiert als: *IFPI*, Recorded Music Sales 2008)

IFPI IFPI Digital Music Report 2008, abrufbar unter www.ifpi.org/content/library/DMR2008.pdf
(zitiert als: *IFPI*, Digital Music Report 2008)

IFPI IFPI Digital Music Report 2009, abrufbar unter www.ifpi.org/content/library/DMR2009.pdf
(zitiert als: *IFPI*, Digital Music Report 2009)

IFPI IFPI Digital Music Report 2010, abrufbar unter www.ifpi.org/content/library/DMR2010.pdf
(zitiert als: *IFPI*, Digital Music Report 2010)

Motion Picture Association of America (MPAA) Theatrical Market Statistics 2007
(zitiert als: *MPAA*, Theatrical Market Statistics 2007)

Organization for Economic Cooperation and Development (OECD) Participative Web and User-Generated Content: Web 2.0, Wikis and Social Networking, 2007, abrufbar unter: http://213.253.134.43/oecd/pdfs/browseit/9307031E.PDF (zitiert als: *OECD*, Web 2.0, 2007)

Music and Entertainment Industries Research Group der University of Hertforshire Music Experience and Behaviour in Young People, 2009, abrufbar unter http://www.ukmusic.org/files/UK%20Music_Uni%20Of%20Herts_09.pdf

Sandvine 2009 Global Broadband Phenomena, Research Report, Executive Summary, abrufbar unter http://www.sandvine.com/downloads/documents/2009%20Global%20Broadband%20Phenomena%20-%20Executive%20Summary.pdf

US Copyright Office The Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary, 1998, abrufbar unter http://www.copyright.gov/legislation/dmca.pdf (zitiert als: US Copyright Office, DMCA Summary, 1998)

Wold, Erling/Blum, Thom/Keislar, Douglas/Wheaton, James Classification, Search, and Retrieval of Audio, 1999, abrufbar unter: http://www.musclefish.com/crc/crcwin.html (zitiert als: *Wold/Blum/Keislar/Wheaton*, Search of Audio, 1999)

Nicht-juristische Literatur: Zeitungs- und Zeitschriftenartikel, Blogs etc.

Anderson, Nate Motion-based analysis can filter copyrighted video clips, Ars Technica, 14.03.2007, abrufbar unter http://arstechnica.com/news.ars/post/20070314-motion-based-analysis-can-filter-copyrighted-video-clips.html

ders. Music exec: „Music 1.0 is dead", Ars Technica, 26.02.2008, abrufbar unter http://arstechnica.com/news.ars/post/20080226-music-exec-music-1-0-is-dead.html

ders. On demand in command: 51% of young Net users view TV online, Ars Technica, 6.8.2009, abrufbar unter http://arstechnica.com/media/news/2009/08/half-of-all-young-internet-users-now-watch-tv-online.ars

Anderson, Kevin Cash for Clicks, The Guardian, 10.08.2009, abrufbar unter: http://www.guardian.co.uk/media/2009/aug/10/paid-content-charging-online

Arrington, Michael Movie Labels To Launch New „Open Market" Play Anywhere Scheme As Last Ditch Effort To Save DRM, TechCrunch, 26.08.2009, abrufbar unter http://www.techcrunch.com/2008/08/26/movie-labels-to-launch-new-open-market-play-anywhere-scheme-as-last-ditch-effort-to-save-drm/

Bangeman, Eric Consortium's user-generated content principles extend far beyond fair use", Ars Technica, 18.10.2007, abrufbar unter http://arstechnica.com/news.ars/post/20071018-consortiums-user-generated-content-principles-extend-far-beyond-fair-use.html

ders. Viacom's true desire: one copyright filter to rule them all, Ars Technica, 22.10.2007, abrufbar unter http://arstechnica.com/news.ars/post/20071022-viacoms-true-desire-one-copyright-filter-to-rule-them-all.html?rel

ders. DRM (on music) is dead. Long live DRM (on video)!, Ars Technica, 08.01.2008, abrufbar unter http://arstechnica.com/news.ars/post/20080108-drm-is-dead-for-music.html

Bonstein, Julia Kundensuche im Feindesland, Der Spiegel, 16/2009, S. 100 ff.

Borland, John RIAA Sues 717 File-Swappers, CNET News, 27.1.2005, http://news.com.com/2110-1027_3-5553517.html

van Buskirk, Eliot Estimates: Radiohead Made Up To $10 Million on Initial Album Sales (Updated), WIRED, 19.10.2007, http://www.wired.com/listening_post/2007/10/estimates-radio/

Chartier, David MySpace inks advertising deal with MTV networks, Ars Technica, 03.11.2008, abrufbar unter http://arstechnica.com/news.ars/post/20081103-myspace-inks-advertising-deal-with-mtv-networks.html

Chen, Steve The state of our video ID tools, The Official Google Weblog, 14.06.2007, abrufbar unter http://googleblog.blogspot.com/2007/06/state-of-our-video-id-tools.html

Cheng, Jacqui Amazon rounds out DRM-free music offering with Sony BMG, Ars Technica, 10.01.2008, abrufbar unter http://arstechnica.com/news.ars/post/20080110-amazon-rounds-out-drm-free-music-offering-with-sony-bmg.html

dies. DVD sales tank in 2009 as Americans head to the cinema, Ars Technica, 04.01.2010, abrufbar unter: http://arstechnica.com/media/news/2010/01/dvd-sales-tank-in-2009-as-americans-head-to-the-cinema.ars

Dale, Chris/ Zamost, Aaron YouTube myth busting, YouTube Biz Weblog, 20.07.2009, abrufbar unter http://ytbizblog.blogspot.com/2009/07/youtube-myth-busting.html

Delaney, Kevin J. YouTube to Test Software To Ease Licensing Fights, The Wall Street Journal, 12.06.2007, abrufbar unter http://online.wsj.com/article/SB118161295626932114.html

Dettweiler, Marco Kein Kopierschutz mehr! Na und?, Computer & Internet, FAZ.NET v. 07.01.2009, abrufbar unter http://www.faz.net/s/Rub4C34FD0B1A7E46B88B0653D6358499FF/Doc~E044C395EA5DE484BBEA50FC047365D26~ATpl~Ecommon~Scontent.html

Dignan, Larry Google moves to show YouTube has „a very credible business model", ZDNet, 17.07.2009, abrufbar unter http://blogs.zdnet.com/BTL/?p=21288

Dong Ngo, Meraki Internet usage via handheld devices soars, CNET News, 18.8.2009, abrufbar unter http://news.cnet.com/8301-1035_3-10312296-94.html

Evans, Brian L. Perceptual Image Hashing – Methods, Image Hashing Research, University of Texas in Austin, abrufbar unter http://users.ece.utexas.edu/~bevans/ projects/hashing/methods.html

von Gehlen, Dirk Warnen statt Klagen: Die Musikindustrie ändert ihre Strategie in Sachen Internet-Piraterie, jetzt.de, 23.12.2008, http://jetzt.sueddeutsche.de/texte/anzeigen/459154

Germain, Jack Dusting for Copyright Clues With Digital Fingerprinting Tech, TechNewsWorld, 22.08.2008, abrufbar unter http://www.technewsworld.com/rsstory/64249.html

Greif, Björn T-Mobile Jukebox verzichtet auf DRM, ZDNET.de, 05.06.2009, abrufbar unter www.zdnet.de/news/lebensart_lifestyle_digital_t_mobile_jukebox_verzichtet_auf_drm_story-39001025-41004968-1.htm

Hansell, Saul Bits Debate: Is Copyright Protection Needed or Futile?, New York Times Weblog, 14.01.2008, abrufbar unter https://bits.WeWeblogs.nytimes.com/2008/01/14/bits-debate-is-copy-protection-needed-or-futile/

Hansen, Sven Gesprengte Ketten – Legale MP3-Downloads in Deutschland, c't 2009, Heft 9, S. 136-141

Harmon, Amy Recording Industry Goes After Students Over Music Sharing, The New York Times, 23.4.2003, S. A1

Harvey, Mike Single-mother digital pirate Jammie Thomas-Rasset must pay $ 80,000 per song, Times Online, 19.06.2009, abrufbar unter http://technology.timesonline.co.uk/tol/news/tech _and_web/article6534542.ece

Hendrickson, Mark YouTube Tries a Little Harder to Protect Copyright Holders, TechCrunch, 15.10.2007, abrufbar unter http://www.techcrunch.com/2007/10/15/youtube-tries-a-little-harder-to-protect-copyright-holders

Hirschberg, Lynn The Music Man, 02.09.2007, The New York Times, abrufbar unter http://www.nytimes.com/2007/09/02/magazine/02rubin.t.html?pagewanted=5&_r=1&ei=5087&em&en=314fd873126f1af6&ex=1189051200

Holahan, Catherine Sony BMG Plans to Drop DRM, businessweek.com, 04.01.2008, abrufbar unter http://www.businessweek.com/technology/content/jan2008/tc2008013_398775.htm

Jobs, Steve Thoughts on Music, 06.02.2007, abrufbar unter http://www.apple.com/hotnews/thoughtsonmusic/

Kane, Margaret Wal-Mart reverses policy on DRM?, CNET News, 10.10.2008, abrufbar unter http://news.cnet.com/8301-1023_3-10063168-93.html?tag=mncol;txt

King, David Latest Content ID Tool for YouTube, The Official Google Weblog, 15.10.2007, abrufbar unter http://googleblog.blogspot.com/2007/10/latest-content-id-tool-for-youtube.html

ders. The Official Google Weblog, Making money on YouTube with Content ID, 27.08.2009, abrufbar unter http://googleblog.blogspot.com/2008/08/making-money-on-youtube-with-content-id.html

Klopp, Tina EU lässt Netzsperren zu, Zeit Online, 12.11.2009, abrufbar unter http://www.zeit.de/digital/internet/2009-11/eu-netzsperren

Kravets, David 10 Years Later, Misunderstood DMCA is the Law That Saved the Web, WIRED, 27.10.2008, abrufbar unter http://Weblog.wired.com/27bstroke6/2008/10/ten-years-later.html

Krazit, Tom YouTube slowly building ad-friendly content, CNET News, 08.05.2009, abrufbar unter http://news.cnet.com/8301-1023_3-10236753-93.html?part=rss&tag=feed&subj=News-DigitalMedia

Li, Kenneth /Auchard, Eric YouTube to test video ID with Time Warner, Disney, Reuters, 12.06.2007, abrufbar unter http://www.reuters.com/article/wtMostRead/idUSWEN871820070612

Marr, Merissa/ Delaney, Kevin J. Disney, Microsoft Lead Copyright Pact", WSJ.com, 19.10.2007, abrufbar unter http://online.wsj.com/public/article_print/SB119269788721663302. html

Müller, Peter Microsoft verlängert DRM für MSN-Music-Songs, iPhone-Welt News, 22.06.2008, abrufbar unter http://www.macwelt.de/artikel/_News/356844/microsoft_verlaengert_drm_fuer_msn_music_songs/1

McCarthy, Caroline ComScore: 100 million YouTube viewers in October, CNET News, 10.12.2008, abrufbar unter http://news.cnet.com/8301-1023_3-10120027-93.html?part=rss&tag=feed&subj=News-DigitalMedia

dies. MTV Networks: which video ads work best, CNET News, 15.7.2009, abrufbar unter http://news.cnet.com/8301-1023_3-110287132-93.html?part=rss&tag=feed&subj=News-DigitalMedia

McDermott, Eileen The great copyright debate, Managing Intellectual Property, March 2009, S. 26 ff.

Pareles, Jon David Bowie, 21st-Century Entrepreneur, The New York Times, 09.06.2002, abrufbar unter http://www.nytimes.com/2002/06/09/arts/music/09PARE.html

Patalong, Frank Kopierschutz ist tot. Amazon komplett DRM-frei, Spiegel Online, 11.1.2008, abrufbar unter http://www.spiegel.de/netzwelt/web/0,1518,527992,00.html

ders. Patalong, DRM – Musik mit Ablaufdatum, Spiegel Online, 24.04.2008, abrufbar unter www.spiegel.de/netzwelt/tech/0,1518,549385,00.html

Rose, Frank Dear Hollywood Studios: Let My Video Go, WIRED, 25.02.2008, abrufbar unter www.wired.com/entertainment/hollywood/magazine/16-03/st_essay

Rosenblatt, Bill 2006 Year in Review: DRM Technologies, DRM Watch, 21.12.2006, abrufbar unter http://www.drmwatch.com/drmtech/article.php/3650401

ders. Thoughts on Notice, Takedown, Fingerprints, and Filtering“, DRM Watch, 15.03.2007, abrufbar unter http://www.drmwatch.com/legal/article.php/3665921

ders. Is EMI’s DRM-Free Strategy Working?, DRM Watch, 08.08.2007, abrufbar unter http://www.drmwatch.com/ocr/article.php/3693316

ders. Amazon Launches DRM-Free Music Service, DRM Watch, 27.09.2007, abrufbar unter www.drmwatch.com/ocr/article.php/3702096

ders. MovieLabs Shows Results of Fingerprint Testing, DRM Watch, 27.09.2007, abrufbar unter http://www.drmwatch.com/watermarking/article.php/3702101

ders. Radiohead Takes the Lead in Race to the Bottom, DRM Watch, 08.11.2007, abrufbar unter www.drmwatch.com/ocr/article.php/3710021

ders. Auditude’s Fingerprinting Powers Contextual Ad Service on MySpace, DRMWatch, 6.11.2008, abgerufen am www.drmwatch.com/watermarking/article.php/3783336

ders. 2007 Year in Review, Part 2, DRM Watch, 27.12.2007, abrufbar unter http://www.drmwatch.com/watermarking/article.php/3718651

ders. New Market Study Predicts Growth in Watermarking and Fingerprinting Markets, 24.01.2008, abrufbar unter http://www.drmwatch.com/watermarking/article.php/3723626

Sandoval, Greg Could peace be near for YouTube and Hollywood?, CNET News, 23.07.2008, abrufbar unter http://news.cnet.com/8301-1023_3-9996905-93.html

ders. NBC finds formula for fighting pricay, CNET News, 23.09.2008, abrufbar unter http://news.cnet.com/8301-1023_3-10048949-93.html?part=rss&tag=feed&subj=News-DigitalMedia

ders. Feature films coming to YouTube, CNET News, 06.11.2008, abrufbar unter http://news.cnet.com/8301-1023_3-10083481-93.html?part=rss&tag=feed&subj=News-DigitalMedia

ders. Dear Steve Jobs: Set the music free, CNET News, 20.11.2008, abrufbar unter http://news.cnet.com/8301-1023_3-10103484-93.html?part=rss&tag=feed&subj=News-DigitalMedia

ders. Universal Music seeing 'tens of millions' from YouTube, CNET News, 18.12.2008, abrufbar unter http://news.cnet.com/8301-1023_3-10126439-93.html?tag=mncol;txt

ders. Universal digital chief on iTunes, DRM, and Android, CNET News, 12.01.2009, abrufbar unter http://news.cnet.com/8301-1023_3-10140244-93.html?part=rss&tag=feed&subj=News-DigitalMedia

ders. SpiralFrog DRM music to play 60 Days, then vanish, CNET News, 20.03.2009, abrufbar unter http://news.cnet.com/8301-1023_3-10201355-93.html?part=rss&tag=feed&subj=News-DigitalMedia

ders. Warner Music Group and YouTube talking again, 10.07.2009, abrufbar unter http://news.cnet.com/8301-1023_3-10284399-93.html?part=rss&tag =feed&subj=News-DigitalMedia

ders. iLike talks download store with music labels, CNET News, 21.07.2009, abrufbar unter http://news.cnet.com/8301-1023_3-10292389-93.html?part=rss&tag=feed&subj=News-DigitalMedia

ders. MPAA: Antipiracy is now „content protection", CNET News, 16.10.2009, abrufbar unter: http://news.cnet.com/8301-31001_3-10376839-261.html?part=rss&tag=feed&subj=News-DigitalMedia

ders. End of the world as Hollywood knows it, CNET News, 20.10.2009, abrufbar unter http://news.cnet.com/8301-31001_3-10378654-261.html

ders. YouTube, Warner Music feud nearing an end, CNET News, 18.09.2009, abrufbar unter, http://news.cnet.com/8301-1023_3-10356764-93.html

Schmidt, Holger Ohne Kopierschutz mehr Umsatz, Frankfurter Allgemeine Zeitung, 03.03.3008, S. 15., abrufbar unter http://www.faz.net/s/RubE2C6E0BCC2F04DD787CDC274993E9C1/Doc~EDCAB4B2561C64E25AAF65B87BB8BF5B8~ATpl~Ecommon~Scontent.html

Schneier, Bruce Cryptanalysis of MD5 and SHA: Time for a New Standard, Computerworld, 19.08.2004, abrufbar unter http://schneier.com/essay-074.html

Schulz, Thomas Schluss mit lustig, Spiegel Online, 05.02.2005, abrufbar unter http://www.spiegel.de/spiegel/print/d-39257707.html

Shinal, John Warner Music's Bronfman on DRM-free tunes. The technology never did what it needed to do, vatornews, 07.11.2008, abrufbar unter http://vator.tv/news/show/2008-11-07-warner-musics-bronfman-on-drm-free-tunes

Steinert-Threlkeld, Tom YouTube's video ID system: is 75 percent good enough?, in: ZDNet Undercover: YouTube's Video Identification System, November 2008

Stone, Brad One Anti-Piracy System to Rule Them All, New York Times, Bits Weblog, 21.09.2007, abrufbar unter http://bits.blogs.nytimes.com/2007/09/21/one-anti-piracy-system-to-rule-them-all/

Theurer, Marcus Die Musikindustrie zweifelt am Kopierschutz, FAZ.NET, 04.06.2004, abrufbar unter http://www.faz.net/s/RubE2C6E0BCC2F04DD787CDC274993E94C1/Doc~EC158BDE6F1404D6D8A8BAD5AA28D1357~ATpl~Ecommon~Scontent.html

ders. Geldregen auf der Bühne, FAZ.NET, 19.09.2007, abrufbar unter http://www.faz.net/s/RubD16E1F55D21144C4AE3F9DDF52B6E19/Doc~E48F4D01A669D48E1A27ACD3A9C87B3CD~ATpl~Ecommon~Scontent.html

ders. Auf der Suche nach der Zukunft, Frankfurter Allgemeine Zeitung, 09.04.2009, S. 21

Timmer, John A decade of the DMCA: keep the Safe Harbor, ditch the rest, Ars Technica, 28.10.2008, abrufbar unter http://arstechnica.com/news.ars/post/20081028-adecade-of-the-dmca-keep-the-safe-harbor-ditch-the-rest.html

Wilkinson, Scott Musical Fingerprints, Electronic Musician, 01.09.2003, http://www.emusician.com/mag/tech/emusic_musical_fingerprints/index.html

Winkelhage, Johannes Apple macht den Weg frei, Frankfurter Allgemeine Zeitung, 08.01.2009, S. 18.

Zack, Shenaz In the future, everyone will monetize their 15 minutes, 25.08.2009, abrufbar unter http://googleblog.blogspot.com/2009/08/in-future-everyone-will-monetize-their.html

Ohne Autor Sony Music Japan verzichtet auf Kopierschutz, heise online, 03.10.2004, abrufbar unter http://www.heise.de/newsticker/meldung/Sony-Music-Japan-verzichtet-auf-Kopierschutz-106635.html

Ohne Autor Google kauft Online-Video-Seite YouTube, heise online, 10.10.2006, abrufbar unter http://www.heise.de/newsticker/meldung/Google-kauft-Online-Video-Seite-YouTube-169658.html

Ohne Autor The End of Free Trade? How YouTube and MySpace will stop users from sharing copyrighted content, Newsweek Web Exclusive, 20.10.2006, abrufbar unter http://www.newsweek.com/id/45365

Ohne Autor EMI beendet die Ära kopiergeschützter CDs, 08.01.2007, gullinews, abrufbar unter http://www.gulli.com/news/emi-beendet-die-ra-kopiergesch-2007-01-08/

Ohne Autor For YouTube, a System to Halt Copyright-Infringement Videos, Associated Press, The New York Times, 28.07.2007, abrufbar unter http://www.nytimes.com/2007/07/28/ business/28google.html

Ohne Autor Fans bestimmen Preis des neuen Radiohead-Albums selbst, heise online, 01.10.2007, abrufbar unter http://www.heise.de/newsticker/meldung/96828

Ohne Autor YouTube startet automatische Video-Identifizierung, heise online, 16.10.2007, abrufbar unter http://www.heise.de/newsticker/meldung/97434

Ohne Autor Kleine Preise bei Apple, sueddeutsche.de, 17.10.2007, abrufbar unter http://www.suedeutsche.de/computer/artikel/605/138322/print.html

Ohne Autor Sorge um Nutzerrechte wegen Copyright-Filter fürs Web 2.0, heise online, 20.10.2007, abgerufen am http://www.heise.de/newsticker/meldung/97678

Ohne Autor Neues Radiohead-Album auf CD und vielleicht bald bei iTunes, heise online, 12.12.2007, abrufbar unter http://www.heise.de/newsticker/meldung/100481

Ohne Autor Warner-Music-MP3 s ab sofort kopierschutzfrei bei Amazon, heise online, 28.12.2007, abrufbar unter http://www.heise.de/newsticker/meldung/101099

Ohne Autor Amazon nimmt DRM-freie Musik von Sony BMG ins Angebot, heise online, 11.01.2008, abrufbar unter http://www.heise.de/newsticker/meldung/101664

Ohne Autor Radiohead-Album erobert auch Platz 1 der US-Charts, heise online, 11.01.2008, abrufbar unter http://www.heise.de/newsticker/meldung/101638

Ohne Autor Sony Pictures proposes Open Market for Movie protection, informitiv.com, 27.08.2008, abrufbar unter http://informitv.com/news/2008/08/27/sonypicturesproposes/

Ohne Autor MySpace und MTV testen neues Vermarktungsmodell für Online-Videos, heise online, 03.11.2008, abrufbar unter http://www.heise.de/newsticker/meldung/118328

Ohne Autor US-Musikindustrie experimentiert mit P2P-Flatrate für Studenten, heise online, 10.12.2008, abrufbar unter http://www.heise.de/newsticker/meldung/120220

Ohne Autor US Musikindustrie gibt Massenklagen auf, heise online, 19.12.2008, abrufbar unter http://www.heise.de/newsticker/meldung/US-Musikindustrie-gibt-Massenklagen-auf-Update-191425.html

Ohne Autor US-Musikindustrie: Das Ende der „Schreckensherrschaft"?, heise online, 20.12.2008, abrufbar unter http://www.heise.de/newsticker/meldung/120789

Ohne Autor Macworld: iTunes-Musik wird vom Kopierschutz befreit, heise online, 06.01.2009, abrufbar unter http://www.heise.de/newsticker/meldung/121237

Ohne Autor Auch Musicload will (fast) vollständig auf digitale Rechteverwaltung verzichten, heise online, 08.01.2009, abrufbar unter http://www.heise.de/newsticker/meldung/121324

Ohne Autor Mediamarkt bietet MP3-Songs ohne DRM an, 29.01.2009, heise online, abrufbar unter http://www.heise.de/newsticker/meldung/126576

Ohne Autor Saturn: 250.000 MP3-Alben für je 5 Euro, 13.03.2009, heise online, abufbar unter http://www.heise.de/newsticker/meldung/134533

Ohne Autor Amazon startet MP3-Downloads in Deutschland, c't news, 01.04.2009, abrufbar unter http://www.heise.de/ct/news/meldung/135554

Ohne Autor United Internet kooperiert mit Amazon MP3, 27.05.2009, heise online, abrufbar unter, http://www.heise.de/newsticker/United-Internet-kooperiert-mit-Amazon-MP3--/meldung/ 139426

Ohne Autor Verband: Download-Markt wächst weiter, c't news, 03.06.2009, abrufbar unter www.heise.de/ct/news/meldung/139798

Ohne Autor T-Mobile bietet kopierschutzfreie Musik-Downloads an, c't news, 07.06.2009, abrufbar unter www.heise.de/ct/T-Mobile-bietet-kopierschutzfreie-Musik-Downloads-an---/news/meldung/140000

Ohne Autor Warner Music und YouTube: Ende der Eiszeit?, heise online, 11.07.2009, abrufbar unter http://www.heise.de/newsticker/meldung141870

Ohne Autor iTunes dominiert weiter den US-Musikmarkt, heise online, 18.08.2009, abrufbar unter http://www.heise.de/newsticker/meldung/143708

Ohne Autor Google will mit Youtube endlich Geld einnehmen, Frankfurter Allgemeine Zeitung, 21.8.2009, S. 17

Ohne Autor Musikindustrie setzt auf Kombi-Angebote und „Three Strikes",heise online, 17.09.2009, abrufbar unter http://www.heise.de/newsticker/meldung/145474

Ohne Autor MySpace startet Musikdienst, 25.09.2008, heise online, abrufbar unter http://www.heise.de/newsticker/meldung/116483

Ohne Autor Soziale Netzwerke vor der Gewinnschwelle, Frankfurter Allgemeine Zeitung, 29.9.2009, S. 23

Ohne Autor YouTube darf wieder Warner-Videos zeigen, 30.09.2009, tagesschau.de, abrufbar unter http://www.tagesschau.de/warnertube100.html

Ohne Autor Zehn Jahre Digital Millennium Copyright Act: Recht fürs Internet?, heise online, 28.10.2008, abrufbar unter http://www.heise.de/newsticker/meldung/118043

Ohne Autor Apple ändert Kurs bei iTunes, Frankfurter Allgemeine Zeitung, vom 08.01.2009, S. 16

Ohne Autor Bericht: YouTube und Warner einigen sich über Musikvideo-Lizenzen, heise online, 29.09.2009, abrufbar unter http://www.heise.de/newsticker/meldung/Bericht-YouTube-und-Warner-einigen-sich-ueber-Musikvideo-Lizenzen-798101.html

Ohne Autor YouTube: Über 1 Milliarde Videoabrufe pro Tag, 11.10.2009, heise online, abrufbar unter http://www.heise.de/newsticker/meldung/YouTube-Ueber-1-Milliarde-Videoabrufe-pro-Tag-821259.html

Ohne Autor Widerstand im EU-Parlament gegen Internet-Sperren bei Urheberrechts verletzungen bröckelt, heise online, 15.10.2009, abrufbar unter http://www.heise.de/ newsticker/meldung/Widerstand-im-EU-Parlament-gegen-Internet-Sperren-bei-Urheberrechtsverletzungen-broeckelt-830015.html

Ohne Autor Schwarz-Gelb gegen Internetsperren bei Urheberrechtsverletzungen, heise online, 19.10.2009, abrufbar unter http://www.heise.de/meldung/Schwarz-Gelb-gegen-Internetsperren-bei-Urheberrechtsverletzungen-832715.html

Ohne Autor Frankreich: Internetsperre für Urheberrechtsverletzer gebilligt, heise online, 22.10.2009, abrufbar unter http://www.heise.de/newsticker/meldung/Frankreich-Internetsperre-fuer-Urheberrechtsverletzer-gebilligt-837138.html

Ohne Autor Studie: Echtzeit-Unterhaltung ist Web-Traffic-Größe Nummer 1, heise online, 26.10.2009, abrufbar unter http://www.heise.de/newsticker/meldung/Studie-Echtzeit-Unterhaltung-ist-Web-Traffic-Groesse-Nummer-1-839567.html

Ohne Autor 36 Million German Internet Users Viewed More Than 6 Billion Videos Online in August 2009, comScore, 27.10.2009, abrufbar unter http://www.comscore.com/ Press_Events/ Press_Releases/2009/10/36_Million_German_Internet_Users_Viewed_ More_Than_6 _Billion_Videos_Online_in_August_2009

Ohne Autor Es gibt keinen Grund, auf ein nationales Urheberrecht zu verzichten – Interview mit Brigitte Zypries, promedia 8/2009, abrufbar unter http://www.promedia-berlin.de/ fileadmin/Archiv/2009/08/promedia200908-online01.pdf

Webseiten (Auswahl)

http://www.alexa.com/siteinfo/thepiratebay.org

http://www.amazon.de/MP3-Musik-Downloads/b/?node=77195031

http://audiblemagic.com/clients-partners/contentsvcs.asp

http://www.bittorrent.com/btusers/help/faq/bittorrent-concepts#4n5

http://www.coral-interop.org

http://csrc.nist.gov/groups/ST/hash/

http://www.facebook.com

http://www.igd.fraunhofer.de

http://isis.poly.edu/projects/percephash

http://www.ipharro.com/all_Images/PDFs/english/iPharro_DAM_ES_1_6_09.pdf

http://www.meinvz.net

http://new.music.yahoo.com/

http://www.myspace.com

http://www.studivz.net

http://www.schuelervz.net

http://www.ugcprinciples.com

http://www.wipo.int/treaties/en/ip/wct/

http://www.wipo.int/treaties/en/ip/wppt/

http://www.youtube.com/