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.