

EUROPEAN BUSINESS SCHOOL
International University Schloss Reichartshausen

These

zur Erlangung des akademischen Grades
Bachelor of Science (B.Sc.)

***Prüfungspflichten und -möglichkeiten
von Host Providern im Hinblick auf Content***

Name: David Dell
Adresse: Waldbachstraße 48, 65347 Eltville (Hattenheim)
Eingereicht bei: Dr. Friedrich Klinkert, RA
Datum: 11. Februar 2008

Inhalt

1.	Einleitung.....	1
1.1.	Problemstellung und Zielsetzung.....	2
1.2.	Gang der Untersuchung.....	2
1.3.	Die Akteure des Internets.....	3
1.4.	Der Hostprovider.....	4
2.	Haftung für Rechtsverletzungen im Internet.....	5
2.1.	Anzuwendendes Recht.....	5
2.2.	Rechtsgrundlagen.....	6
2.2.1.	Straftaten.....	6
2.2.2.	Allgemeine Persönlichkeitsrechte.....	7
2.2.3.	Markenrecht.....	8
2.2.4.	Urheberrecht.....	9
2.2.5.	Weitere Anspruchsgrundlagen.....	10
2.3.	Haftung des Hostproviders.....	10
2.3.1.	Haftung als Täter oder Teilnehmer.....	11
2.3.2.	Haftung als Störer.....	11
2.3.3.	Schutz des Hostproviders durch das Telemediengesetz.....	13
2.4.	Zwischenergebnis: Inhaltsüberwachung als mögliche Folge.....	14
3.	Wirtschaftliche Implikationen.....	15
3.1.	Beeinträchtigung der Rechte des Markeninhabers.....	15
3.2.	Beeinträchtigung der Rechte des Urhebers.....	17
3.3.	Vermeidungskosten für den Hostprovider.....	19
3.3.1.	Löschung bestehender Inhalte.....	19
3.3.2.	Unterlassung von Wiederholungen.....	20
3.3.3.	Verhinderung von Erstbegehung.....	22
3.3.4.	Sonderfall: Handeln im geschäftlichen Verkehr.....	23
3.4.	Zwischenergebnis: Schaden und Vermeidungskosten.....	23
4.	Abwägung.....	24
4.1.	Generelle Zumutbarkeit.....	24
4.2.	Verbot der totalen Inhaltsüberwachung.....	26
4.3.	Stellenwert des Rechtsschutzes gegenüber modernen Geschäftsmodellen.....	26
4.4.	Zwischenergebnis: Sinnvolle Prüfung.....	27
5.	Fazit und Ausblick.....	28
	Literatur.....	30
	Anhang: Fallstudien.....	34

1. Einleitung

In der populären Meinung wird die Institution des Internets vielfach fälschlicherweise als rechtsfreier Raum wahrgenommen. Geprägt durch die vermeintliche Anonymität und die unüberschaubare Vielzahl seiner Akteure, hat es mehr den Anschein einer anarchistischen Spielweise, als den eines seriösen Mediums. Doch tatsächlich prägt das Internet wie kaum eine andere Innovation Wirtschaft, Recht und unser alltägliches Leben. Tagtäglich werden unter Zuhilfenahme des Internets hunderttausende gültige Geschäfte geschlossen. Die Realität des Internets als Multimillionen-Euro-Marktplatz wird mit Blick auf die Börse mehr als deutlich. Die Investitionssummen, welche, vorbei am Durchschnittsnutzer, für Anteile an Internetfirmen gezahlt werden, sind gewaltig (Ebay -> Alando.de: 43 Millionen US-Dollar, 1999; Google -> Youtube: 1,65 Milliarden US-Dollar, 2006; Microsoft -> Facebook: 240 Millionen US-Dollar für 1,6 Prozent der Anteile, 2007). Das Internet fügt sich nahtlos in die Reihe der wichtigsten Basisinnovationen der Menschheit ein. Es steht neben der Dampfmaschine und der Entdeckung der Elektrizität (Devezas et al., 2005).

Doch wie jede Innovation offenbart auch das Internet zuvor unbekannte Problemfelder. Im Internet werden alltäglich reale Straftaten und unerlaubte Handlungen begangen und real existierende Rechte verletzt. Entweder fehlt oft die Sensibilisierung dafür, dass eine Handlung im Internet genauso real und folgenreich ist wie jede andere Handlung auch (siehe auch Balestrino, 2007), oder aber die Anonymität in der Masse verheißt relativ risikofreie Gewinne durch bewusst illegales Handeln (siehe auch Burden / Palmer, 2003).

Es gilt, einen schmalen Grad zu finden zwischen den Segnungen in Form neuer Vertriebswege und den Gefahren der Innovation Internet. Die Frage der Verantwortung ist hier so maßgeblich und zweischneidig wie in keinem anderen Medium. Zweifelsfrei wird jeder der Meinung sein, dass gemäß den Normen unserer Gesellschaft, derjenige, der eine schadhafte Handlung ausführt, auch die Konsequenzen zu tragen hat. Weitergehend würde man Zustimmung erhalten, auch Gehilfen des Übeltäters in die Verantwortung zu ziehen. Doch gerade dieser Abgrenzung des Täterkreises steht die Funktionsweise des Internets entgegen. Die Vielzahl von Ebenen, die ein Inhalt im Internet durchläuft und die gewaltige Menge an Informationen, die an bestimmten

Schaltstellen zusammenlaufen, erzeugen eine Grauzone, in der an dem in Frage stehenden Rechtsbruch in der einen oder anderen Form mitgewirkt wird.

1.1. Problemstellung und Zielsetzung

Die Kernfrage lautet inwieweit denjenigen, der im Internet Rahmenbedingungen für eine Vielzahl nutzenstiftender Vorgänge schafft, aber damit gleichzeitig auch die Möglichkeit zu vielfachem Rechtsbruch bietet, eine Schuld trifft. Weiterhin, welche Möglichkeiten ihm zu Gebote stehen, Rechtsbrüche zu erkennen und zu verhindern und so einer Haftung zu entgehen.

Diese Arbeit soll entsprechend der vorgenannten Fragestellung die aktuelle rechtliche Situation und Diskussion in Deutschland bis Januar 2008 darstellen, um anschließend eine Abwägung zwischen der Durchsetzung rechtmäßiger Ansprüche gegen so genannte, und dem wirtschaftlichen Interesse von so genannten „Host Providern“ zu treffen.

1.2. Gang der Untersuchung

Nachdem eine Übersicht über die verschiedenen Akteure im Internet geschaffen und der Begriff des Host Providers definiert wird, wird im ersten Teilbereich dieser Arbeit durch Rückgriff auf Fachliteratur und Rechtsprechung dargelegt, woraus sich eine Prüfungspflicht des Host Providers ergeben kann. Besonders werden die Schutzwirkung des Telemediengesetzes und deren Auslegung in höchstrichterlicher Rechtsprechung besprochen.

Im zweiten Teil werden durch Betrachtung der Praxis die Implikationen dieser Rechtslage verdeutlicht. Zuerst werden die Schutzwürdigkeit der verletzten Rechte und die Höhe der erlittenen Beeinträchtigungen bewiesen. Dann wird erörtert, welche tatsächlichen Prüfungsmöglichkeiten der Host Provider angesichts der Menge an Informationen die bei ihm zusammenlaufen unter Betrachtung der technischen Realisierbarkeit und Wirtschaftlichkeit hat.

Im dritten Teil wird eine Abwägung zwischen dem Rechtsanspruch Dritter und dem Anspruch des Host Providers und der Allgemeinheit an der Funktion seines Geschäftsmodells getroffen. Es soll geklärt werden, bis zu welchem Grad dem Host Provider eine

bisher nicht genau definierte Prüfungspflicht zugemutet werden kann und nach höheren Grundsätzen zugemutet werden darf.

Im letzten Teil wird ein abschließendes Fazit gezogen, welches Antwort auf die Problemstellung und weiterhin auf die praktische Frage gibt, wie sich ein Hostprovider angesichts seiner Verantwortung zu Verhalten hat.

1.3. Die Akteure des Internets

Wenning (1998), welcher den Begriff der „Akteure des Internets“ prägte, unterteilt diese anhand der technischen Ebenen, welche ein Inhalt bei der Übertragung durch das Internet durchläuft. Diese Ebenen sind:

1. Content-Providing: Der Ersteller und/oder Initialsender eines Webinhalts ist der so genannte Contentprovider.
2. Host-Providing: Der Hostprovider stellt dem Contentprovider Speicherplatz im Netz (Webspace) zur Verfügung und hält dessen Inhalte zum Abruf bereit.
3. Access-Providing: Der Accessprovider speist die Inhalte in das Internet ein.
4. [...] Die Inhalte stehen nun im Internet zur Verfügung.
5. Access-Providing 2: Ein weiterer Accessprovider leitet die Information zum Rezipienten weiter.
6. Rezipient: Der Rezipient kann sich die angeforderten Inhalte anzeigen lassen.

in Anlehnung an Wenning (1998) Abs. 6

Bereits beim Betrachten dieser Darstellung wird deutlich, dass eine statische Einordnung eines Akteurs in einen dieser Bereiche nicht möglich ist. Vielmehr kann die gleiche Person oder Gesellschaft gleichzeitig Host- sowie Accessprovider sein. Zahlreiche Webseiten bieten zudem sowohl eigenen Inhalt an - wären hier also Contentprovider - als auch die Möglichkeit für Nutzer, Inhalte zu erstellen (z. B. die Möglichkeit einzelne Artikel zu kommentieren), womit sie die Funktion eines Hostproviders einnehmen. Somit lässt sich eine Zuordnung immer nur entsprechend des konkret in Frage stehenden Sachverhaltes tätigen.

Paragraph 2 des Telemediengesetzes bleibt die Unterscheidung zwischen Host-, Content- und Accessprovider schuldig und kennt nur die Bezeichnung „Dienstanbieter“ unter welcher diese drei zusammengefasst werden. Jedoch ergibt sich eine Unterscheidung zwingend aus den §§ 8-10, in denen von „fremden“ oder „durchgeleiteten“ Informationen die Rede ist.

1.4. Der Hostprovider

Der Begriff „Host“ steht im Englischen für Gastgeber, Veranstalter und Wirt. Der Hostprovider hält also gleich einem Wirt Inhalte Dritter zum Abruf bereit. Noch vor einigen Jahren beschränkte sich dieses zumeist lediglich auf das Zur-Verfügung-Stellen von Speicherplatz auf dem Server des Hostproviders, welcher die Inhalte von jedem internetfähigen Rechner nach Eingabe der individuellen Web-Adresse abrufbar machte. Der Ersteller der Inhalte musste eine gewisse technische Versiertheit aufweisen, um die Daten auf den Server seines Hostproviders zu übertragen und er musste zuvor die Webseite selbst entsprechend der Webstandards programmieren.

Im Rahmen des Wandels zum Web 2.0, welches von so genanntem User-Generated-Content (engl. „Vom Nutzer erstellter Inhalt“) lebt, wurde es zunehmend einfacher, eigene Inhalte im Netz abzulegen. Der Hostprovider vermischt sich zunehmend mit dem Contentprovider. So bereitet er beispielsweise Inhalte eines Fremden auf und gliedert sie in das Gestaltungsmuster seiner eigenen Webseite ein, über welche der Inhalt dann auch einfach aufzufinden ist. Eine weitere Entwicklung des Webs 2.0 ist, dass diese neue Form des Hostings meist für den Nutzer kostenlos ist und stattdessen über Werbeanzeigen finanziert wird.

Ein gutes Beispiel hierfür ist myspace.com. Auf dieser Webseite, die heute auf Platz 6 der täglich am häufigsten aufgerufenen Webseiten der Welt rangiert (alexa.com, 15.01.2007), hat jeder Internetnutzer nach einfacher Anmeldung ohne Identitätsüberprüfung die Möglichkeit, seine eigene Webseite zu erstellen. Hierfür ist keinerlei technisches Wissen vonnöten. Die eingegebenen Informationen werden von myspace automatisch weiterverarbeitet und stehen „eine technische Sekunde“ (siehe auch OLG Köln v. 18.03.2005 - 6 U 12/01, AI2b) später geordnet und graphisch aufbereitet zur Verfügung. Da jeder fremde Inhalt ohne menschliche Überprüfung, passiv und automatisch (Spindler, 2002, S. 922) verarbeitet und veröffentlicht wird, lässt sich

myspace.com dennoch als Hostprovider bezeichnen, auch wenn die fremden Inhalte neben den eigenen auf der eigenen Webseite dargestellt werden.

Der Hostprovider ist also eine Untergruppe der Internetdienstleister. Ohne Hostprovider wäre das Internet nicht das freie Meinungsforum, in dem jeder sozusagen seine eigene „Kundgebungsfläche“ mieten kann. Die Veröffentlichung von Inhalten wäre großen Unternehmen vorbehalten, welche in der Lage sind, eigene Server zu betreiben.

2. Haftung für Rechtsverletzungen im Internet

Natürlich ist das Internet keinesfalls ein rechtsfreier Raum. Vielmehr gelten für Handlungen im Internet die gleichen zivil- und strafrechtlichen Maßgaben wie für jede andere Handlung auch. Jemand, der im Internet andere beleidigt oder verbotene Schriften verbreitet, muss sich den gleichen Konsequenzen unterwerfen wie in jedem anderen Medium. Allerdings birgt das Internet bei der praktischen Anwendung dieser Normen zahlreiche Probleme.

Da es sich beim Internet um ein weltumspannendes Netzwerk handelt, ist zuerst zu klären, welche nationalen Rechte bei der Bewertung einer Handlung zugrunde zu legen sind (2.1). Nur wenn in diesem Recht entsprechende Anspruchgrundlagen oder Sanktionen existieren, können diese auch im Internet angewendet werden (2.2).

Das nächste Problem ist die technisch bedingte Anonymität des Internets. Im Medium Internet stellt es sich als weitaus schwieriger dar als in jedem anderen Medium, den eigentlichen Täter ausfindig zu machen. Aus reinem Pragmatismus liegt eine Ausweitung des Täterkreises unter Einbeziehung Dritter, welche einfacher zu identifizieren sind und dennoch großen Einfluss auf die Geschehnisse ausüben, nahe (2.3). Die Möglichkeit, den Hostprovider in die Verantwortung zu ziehen, kann legitim sein, ist aber, wie sich später herausstellen wird, zu Recht eingegrenzt (2.4).

2.1. Anzuwendendes Recht

Eine Antwort zur Frage gibt der Gesetzgeber § 3 des Telemediengesetzes. Hier wird grundsätzlich festgelegt, dass der Dienstleister (also auch der Hostprovider), der in Deutschland niedergelassen ist, den Anforderungen des Deutschen Rechts unterliegt. Es

ist zu beachten, dass im selben Paragraphen unter Abs. 4 Nr. 6 das Urheberrecht und verwandte Schutzrechte (also auch das Markenrecht) von dieser Regelung ausgenommen sind. Für diese Rechte gilt das so genannte Schutzlandprinzip. Dies bedeutet, dass „das nationale Recht desjenigen Staates zur Geltung kommt, in dem die Rechtsverletzung begangen wurde“ (Heckmann, 2007, S. 34).

In der Praxis führt beides jedoch zum selben Ergebnis, da eine Markenverletzung einer in Deutschland geschützten Marke immer in Deutschland begangen wird, sofern das Angebot einen wirtschaftlich relevanten Inlandsbezug aufweist (BGH v. 13.10.2004 - I ZR 163/02, b). Hiervon ist bei den meisten in Deutschland niedergelassenen Host Providern auszugehen.

In Bezug auf die Frage des zuständigen Gerichtes innerhalb Deutschlands taucht das Problem des „fliegenden Gerichtsstandes“ auf. Es entsteht dadurch, dass „Tatort“ im Internet jeder Ort sein kann, von dem der in Frage stehende Inhalt abgerufen werden kann. Dies wäre in der Theorie jeder Ort der Welt. Dieser Willkür wurde jedoch durch die Rechtsprechung Einhalt geboten; so kann sich der Kläger den Gerichtstand nicht beliebig aussuchen, sondern ist auch wiederum an die Gebiete gebunden, in denen sich die Verletzungshandlung bestimmungsgemäß auswirken soll (OLG Bremen v. 17.02.2000 - 2 U 139/99).

2.2. Rechtsgrundlagen

In diesem Teil soll noch keine rechtliche Wertung den Host Provider erfolgen. Es soll lediglich der Rahmen des Deutschen Rechtes erläutert werden, gegen den Handlungen im Internet grundsätzlich gewertet werden können.

2.2.1. Straftaten

Da sich Inhalte über das Internet nahezu kostenfrei vervielfältigen und einer unbegrenzten Anzahl an Personen zugänglich machen lassen, zieht dieses Medium naturgemäß auch die Verbreitung von illegalen Inhalten an. Das Strafgesetzbuch (StGB) bezieht diese digitalen Inhalte in § 11 Abs. 3, namentlich als Schriften, in die darauf folgenden Tatbestände ein.

Besonders die nach § 184-184b StGB verbotene Verbreitung von pornographischen Schriften steht immer wieder in der öffentlichen Aufmerksamkeit (Welt Online,

19.10.2007; Spiegel Online, 23.10.2007, 16.05.2007, 23.04.2007; Süddeutsche Zeitung 14.02.2007; Focus Magazin, 12.02.2007). Auch hier hat der Gesetzgeber in § 184c StGB nochmals klar definiert, dass der Tatbestand auch bei der Nutzung von Medien-Telediensten erfüllt bleibt. Die Verbreitung legaler Pornographie (welche nicht unter §§ 184 a+b StGB fällt) über das Internet ist nur dann gestattet, wenn sichergestellt ist, dass nur Volljährige Zugriff auf die Inhalte haben. Die Auslegung dieser „Sicherstellung“ durch die Rechtsprechung ist sehr streng, so reicht es beispielsweise nicht aus, eine Personalausweisnummer abzufragen (BGH v. 19.10.2007 - I ZR 102/05).

Da nie zweifelsfrei festgestellt werden kann, wer letztendlich Inhalte im Internet abrufen oder Geschäfte im Internet abschließt, kommt es häufig zu Straftaten entsprechend § 27 Jugendschutzgesetz (JuSchG). So werden im Internet nach § 15 JuSchG jugendgefährdende Filme und Computerspiele zahlreich ungeschützt zum Verkauf oder Download angeboten (Jugendschutz.net, 2007, S.13). Der BGH hat bestätigt, dass sich die bestehenden Regelungen naturgemäß auch auf den Vertrieb über das Internet anwenden lassen (BGH v. 12.07.2007 - I ZR 18/04).

Die einfache, kostengünstige und relativ anonyme Kommunikation über das Internet kann außerdem Straftaten der §§ 130 bis 131 StGB (Volksverhetzung, Anleitung zu einer Straftat und Gewaltdarstellung) fördern. Nicht nur spezialisierte Internetseiten bieten rechtsradikalen und anderen gewaltbereiten Gruppen ein Forum zur verbotenen Volksverhetzung. Da den Nutzern auf vielen Webseiten die Möglichkeit gegeben wird, Inhalte zu kommentieren, bzw. miteinander zu diskutieren, können sich leicht nach § 130 verbotene Aussagen einschleusen. Informationsseiten zu Amokläufen und Waffenbau leiten die Nutzer weiterhin nach § 130a verbotenerweise zu Straftaten an. Inzwischen sind die zahlreichen über das Internet angebotenen Anleitungen zum Bombenbau zu allgemeiner Bekanntheit gelangt (Suchstring „Anleitung zum Bombenbau“ in der Suchmaschine google.de liefert 1.680 Ergebnisse, 16.01.2001). Die denkbaren und tatsächlichen Verstöße sind unzählige.

2.2.2. Allgemeine Persönlichkeitsrechte

Das Internet bietet besondere Problemfelder im Hinblick auf das Namensrecht (z. B. Domainnamenvergabe) und das Recht auf informationelle Selbstbestimmung (Datenschutz). Jedoch soll es aufgrund ihres Umfangs hier bei der einfachen Nennung

bleiben. Auf Verletzung der besonderen Persönlichkeitsrechte des Urhebers und des Markeninhabers soll im nächsten Absatz gesondert eingegangen werden.

Bei Ehrverletzungen, beispielsweise durch Schmähkritik in Internetforen, ergeben sich bei der rechtlichen Handhabung, wie auch bei den Straftaten festgestellt wurde, keine Unterschiede zu anderen Medien (Wurster, 2001, Abs. 21). Lediglich ist im Internet häufiger aus den in 2.2.1 genannten Gründen mit einer solchen Rechtsverletzung zu rechnen.

2.2.3. Markenrecht

Der Warenaustausch über das Internet in Deutschland wuchs in den letzten Jahren stetig, zuletzt auf ein Volumen von rund 16 Milliarden Euro im Jahr 2006 (Quelle: Jupiter Research, 2006). Es lässt sich annehmen, dass sich unter diesen Waren zahlreiche Plagiate und Reimporte befanden. Das Bundeskriminalamt schreibt bereits im Lagebericht 2001 hierzu: „Im Internet werden vermehrt die sog. Auktionshäuser (z. B. "eBay", "Ricardo") frequentiert, über die erhebliche Mengen [...] abgesetzt werden.“

Eine Verbreitung von Plagiaten oder Reimporten widerspricht dem ausschließlichen Recht des Markeninhabers aus § 14 Markengesetz (MarkG), die Marke zu nutzen und lässt einen Unterlassungsanspruch nach Abs. 5 entstehen. Verschulden wird nicht vorausgesetzt, er „besteht gegen jeden der die rechtswidrige Benutzung [der Marke] durchführt oder begünstigt“ (Gottschalk, 2002, S. 483). Kommt schuldhaftes Handeln (nach § 276 BGB Abs. 2) hinzu, kann ebenfalls ein Schadensersatzanspruch gemäß Abs. 6 (§ 14 MakG) geltend gemacht werden. Bemerkenswert ist die Einbeziehung eines Betriebsinhabers für schuldhaftes Handeln seiner Angestellten nach Abs. 7.

Ein Anspruch auf Vernichtung der angebotenen Ware und aller weiteren, unerlaubter Weise markierten Gegenstände im Besitz des Verletzers ergibt sich aus § 18 MarkG. Dieser hat nach § 19 MarkG auch Auskunft über die Herkunft der Waren zu erteilen (jedoch nicht im unerheblichen Einzelfall). Die genannten Tatbestände können zusätzlich eine strafrechtliche Konsequenz nach sich ziehen (§ 134 MarkG). Es sind hier Freiheitsstrafen bis zu drei beziehungsweise fünf Jahren für gewerbsmäßigen Handel vorgesehen.

Wichtig ist, dass sich das Markenrecht grundsätzlich nur auf solche Handlungen erstreckt, die sich im geschäftlichen Verkehr ereignen mit der Maßgabe im Bezug auf

Handlungen im Internet, dass geschäftlich auch der handelt, der „Privateigentum verkauft, wenn dieser Verkauf einen gewissen Umfang annimmt“ (LG Berlin v. 9.11.2001 - 103 O 149/01).

2.2.4. Urheberrecht

Die bei den Straftaten (2.2.1) erwähnte Erleichterung der Vervielfältigung und Verbreitung von Inhalten durch die Innovation Internet schlägt sich, möglicherweise so stark wie in keinem anderen Feld, auch im Bereich des Urheberrechts nieder. War das Raubkopieren von Musikstücken, Filmen und ähnlichem noch vor 10 Jahren professionell organisierten Banden vorbehalten, wurden in den letzten Jahren ansonsten rechtstreue Bürger zu Urheberrechtsverletzern. In den Jahren 1998 bis 2005 stieg die Zahl der in Deutschland eingeleiteten Strafverfahren in diesem Bereich von 426 auf 2549 (Quelle: GVU, 2006, S. 8). Sie ist seitdem rückläufig (1834 in 2006 (Quelle: s. O.)), was auf größere Sensibilisierung (siehe auch Balestrino, 2007) für den Rechtsbruch zurückzuführen sein könnte (z. B. durch Anti-Raubkopierer-Kampagnen). Traditionell werden in einem Zug mit Urheberrechtsverletzungen im Internet die - auch außerhalb der Szene inzwischen zu Bekanntheit geratenen - P2P-Netzwerke (Peer-to-Peer) genannt (u. a. Seyfert; Taeger/Wiebe; Solmecke, alle 2006). Allerdings werden zunehmend auch die zahlreichen Videohosting-Seiten (z. B. myvideo.de als größter Deutscher Anbieter) bewusst oder unbewusst zum Urheberrechtsbruch genutzt. Auf diesen Seiten können Videos beliebigen Formates hochgeladen werden und stehen automatisch für jeden zum Abruf bereit. Gerade bei den Nutzern dieser Seiten scheint die Sensibilisierung extrem schwach ausgeprägt. Ein Verstoß mündet zudem nur selten in einer Strafverfolgung und damit in Aufnahme in die Statistik. Weiterhin werden Online-Auktionen verwendet, um geschütztes Material unerlaubt zu verkaufen. Im Jahr 2006 entdeckte die Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e. V. 401 Auktionen dieser Form (GVU, 2006, S. 17).

Die oben genannten Formen des unbefugten Verbreitens geschützter Werke widerspricht dem Bestimmungsrecht des Urhebers aus § 12 Urheberrechtsgesetz (UrhG). Es begründet, gleich dem Markenschutz, einen Unterlassungs-, sowie Schadensersatzanspruch bei schuldhaftem Handeln (§ 97 UrhG), einen Vernichtungsanspruch (§ 99 UrhG) und einen Anspruch auf Auskunft über die Herkunft des Werkes, bzw. dessen Vervielfältigung. Der Auskunftsanspruch ist zusätzlich zur Ausnahme des

unerheblichen Einzelfalls (wie im Markenrecht) noch weiter eingeschränkt und nur begründet, wenn die Handlung im geschäftsmäßigen Verkehr stattfand.

2.2.5. Weitere Anspruchsgrundlagen

Dem unter Straftaten (2.2.1) bereits erwähnten Urteil des BGH (I ZR 18/04), in dem die Verbreitung von jugendgefährdenden Medien über die Ebay-Auktionsplattform beurteilt wurde, kommt auch wettbewerbsrechtliche Bedeutung zu. Das Gericht hat klargestellt, dass ein Verstoß gegen Verkaufsbeschränkungen aus dem JuSchG eine unlautere Wettbewerbshandlung, nach § 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG), gegen die Interessen des Verbrauchers darstellt. Ebay ist als Anbieter eines Marktplatzes seinen Verkehrsicherungspflichten nicht nachgekommen. Das zieht somit auch die in diesem Gesetz vorgesehenen Rechtsfolgen nach sich (§§ 8-11 UWG).

2.3. Haftung des Hostproviders

Alle Akteure des Internets, die mit unerlaubten Inhalten in Berührung kommen, stehen in ständiger Gefahr als Beteiligte an einer Straftat, oder aber als Schuldner eines zivilrechtlichen Anspruches zur Verantwortung gezogen zu werden. Um hier eine gewisse Rechtssicherheit zu schaffen und gleichzeitig das Funktionieren der neuen Nutzungsmöglichkeiten des Internets zu garantieren, hat der Gesetzgeber versucht, die entstandenen Problemfelder einheitlich zu regeln.

Erstmals geschah dies mit dem Teledienstgesetz (TDG) vom 22. Juli 1997. Auch das Interesse der Europäischen Gemeinschaft an einheitlichen Regelungen hat sich in der E-Commerce Richtlinie vom 8. Juni 2000 (2000/31/EG) manifestiert, welche durch das bestehende TDG, vor allem in Hinblick auf die Providerhaftung, bereits in innerstaatliches Recht umgesetzt war (Heckmann 2007, S. 159). Das TDG wurde am 01.03.2007 durch das Telemediengesetz (TMG) abgelöst. In dieses neue Gesetz wurden die zentralen Normen des TDG wortlautgleich übernommen. Der Hauptnutzen des neuen Gesetzes ist wohl darin zu sehen, dass es Regelungen, die vormals über mehrere Normenwerke verteilt waren in einem einzigen bündelt (z. B. Aufnahme der Regelungen zum Datenschutz aus dem Medienstaatsvertrag, siehe auch Jäger, 2007).

2.3.1. Haftung als Täter oder Teilnehmer

Unstrittig ist, dass der Verbreiter eigener Inhalte (Contentprovider) gemäß den allgemeinen Grundsätzen die rechtlichen Konsequenzen zu tragen hat. Hieran ändern auch die Regelungen des TMG (beziehungsweise TDG a. F.) nichts (Stadler, 2005, S. 47; § 7 TMG). In diese Täter- oder Gehilfenstellung (unmittelbare Passivlegitimation), welche für die meisten Anspruchsgrundlagen notwendig ist, tritt der Hostprovider jedoch meist nicht ein, da er selbst keine Handlung ausführt. Die einzige Möglichkeit hierzu besteht, wenn er sich die Inhalte zu eigen macht (analog zum Presserecht, Säcker, 2001), indem er sie beispielsweise manuell prüft und eingibt bzw. freischaltet. Im Urheberrecht könnte der Hostprovider auch durch eigene Verletzung des § 97 UrhG unmittelbar passiv legitimiert sein, da er es ist, der die Werke öffentlich zugänglich macht. Volkmann verneint dies jedoch in den meisten Fällen zu Recht (Volkmann, 2005, S. 73ff.).

Eine andere Möglichkeit, den Hostprovider in der Täterstellung zu sehen, ist das Verletzen der unter 2.2.5 angesprochenen Verkehrssicherungspflicht. Ebay kann die Verletzung zugerechnet werden (vor allem aufgrund der finanziellen Beteiligung an den Auktionen). Ein Verschulden, welches von § 823 BGB gefordert wird, ist allerdings nicht mit der E-Commerce Richtlinie vereinbar (siehe Erwägungsgrund 41: „passive Tätigkeit“).

Die Stellung des Hostproviders als Täter oder Teilnehmer ist somit nur schwierig zu begründen, damit fehlt oft der direkte Anspruch aus einer Rechtsverletzung.

2.3.2. Haftung als Störer

Für den Hostprovider ist die mögliche Haftung als Störer von weitaus größerer Bedeutung. Der Störerbegriff leitet sich aus § 1004 des Bürgerlichen Gesetzbuches (BGB) her. Dieser Paragraph ist Bestandteil des Sachenrechts und schützt dem Wortlaut nach das Eigentum vor Beeinträchtigung durch den Störer. Es wird dem Gestörten ein Beseitigungsanspruch garantiert und dieser kann, sind weitere Störungen zu befürchten, auch auf Unterlassung klagen. Einige Normen des BGB beziehen ausdrücklich auch andere Rechte als das Eigentum in den Schutzbereich des § 1004 ein (§ 1027, § 1065, § 1227 BGB). Die Ansprüche gelten also auch bei der Beeinträchtigung aller anderen absoluten Rechte (AG Brakel v. 11.02.1998 - 7 C 748/97), somit auch jener der gewerblichen Schutzrechte. Folglich kann beispielsweise ein Markeninhaber eine

„Mittelsperson“, die an einer unerlaubten Nutzung seiner Marke mitwirkt, als Störer seines exklusiven Rechtes diese Marke zu benutzen, in Anspruch nehmen (BGH v. 19.04.2007 – I ZR 35/04). Für die Geltendmachung einiger gewerblicher Schutzrechte wird jedoch ein Handeln im geschäftlichen Verkehr vorausgesetzt. Bei der Störerhaftung ist zu beachten, dass dieses Kriterium nicht der Störer, sondern der eigentliche Täter erfüllen muss.

Störer kann jede Person sein, die willentlich und adäquat-kausal die Rechtsbeeinträchtigung hervorgerufen hat (BGH v. 10.10.96 - I ZR 129/94). Im Störer muss aber nicht die alleinige Ursache für diese liegen und es muss ihn auch kein Verschulden treffen. Es genügt, wenn der „ihm zurechenbare beeinträchtigende Zustand auf seiner Willensentscheidung“ beruht (Volkman, 2005, S. 61). Auf den ersten Blick scheint der Kreis dieser mittelbaren Störer sehr weit gefasst, darf aber sicherlich nicht unverhältnismäßig auf Dritte erstreckt werden. Die Rechtsprechung setzt hier verschiedene Einschränkungen an. Besonders die Erkennbarkeit der Rechtsverletzung für den vermeintlichen Störer und die Möglichkeit, diese abzustellen sind grundlegend. Es stellt sich nun die Frage, inwieweit der Hostprovider hier einzubeziehen ist.

Der Bundesgerichtshof ist in der Entscheidung *ambiente.de* zu dem Schluss gekommen, dass eine Prüfungspflicht verletzt sein muss (BGH v. 17.05.2001 – I ZR 251/99). Diese Prüfungspflicht wurde stark zugunsten des Hostproviders (hier die Deutsche Vergabestelle für Domainnamen, DENIC) ausgelegt: Das Ausmaß der Prüfung ist unter Betrachtung der Umstände und Zumutbarkeit anzusetzen. In diesem Fall bedeutete dies konkret, dass automatisierte Vorgänge komplett ausgenommen wurden und eine Prüfung durch den Hostprovider nur dann geboten war, wenn er auf die Rechtsverletzung aufmerksam gemacht wurde. Einzig für den Fall, auf den er aufmerksam gemacht wurde, tritt der Hostprovider in die Mitstörerstellung und muss die gebotenen Rechtsfolgen tragen, also den Domainnamen gegebenenfalls freigeben. Es ist allerdings zu bedenken, dass die DENIC nur bedingt als Hostprovider zu verstehen ist, da sie lediglich Internetadressen vergibt und damit einer für das Funktionieren des Internets bedeutsamen Aufgabe nachkommt. In der Entscheidung *ricardo.de* des Bundesgerichtshofes (BGH v. 11.03.2004 – I ZR 304/01), die prägend für Hostprovider der web2.0-Generation ist, wurde die Ansicht darum so nicht fortgeführt. Hier bestand das Gericht ausdrücklich darauf, dass die sich eine Prüfungspflicht auch auf das Verhindern weiterer gleicher Rechtsverletzungen erstreckt.

Der Hostprovider ist also nunmehr auch für zukünftige (und automatisierte) Verletzungen Mitstörer, wenn er nicht entsprechende Prüfungsmaßnahmen ergreift. Das Gericht lässt offen wie diese Prüfungsmaßnahmen im konkreten Fall aussehen müssen und beschränkt sich auf die Bezeichnung „technisch möglich und zumutbar“. Dieser Wortlaut stammt aus dem Gesetzesentwurf zum Teledienstgesetz (BT-Drucksache 14/6098, S. 23). Dort wird weiter ausgeführt, dass die Zumutbarkeitsgrenze jeweils im Einzelfall und in Abhängigkeit von der Wertigkeit des gefährdeten Rechtsgutes zu bestimmen ist.

2.3.3. *Schutz des Hostproviders durch das Telemediengesetz*

Durch § 10 Telemediengesetz (TMG) genießt der Hostprovider, welcher als Dienstanbieter lediglich fremde Informationen für die Nutzer speichert, einen besonderen Schutz. Er ist dem Wortlaut des Gesetzes nach nicht für fremde Informationen „verantwortlich“, wenn er keine Kenntnis von der Rechtsverletzung hat. Dies gilt grundsätzlich sowohl für Straftaten als auch für zivilrechtliche Ansprüche mit der Maßgabe, dass ihm zum Schutz vor zivilrechtlichen Schadensersatzansprüchen auch keine hinweisenden „Tatsachen oder Umstände“ bekannt sein dürfen.

Die hier genannte positive Kenntnis ist nicht mit der „Erkennbarkeit“ der Störerhaftung zu verwechseln, vielmehr geht es um das konkrete Kennen des Inhaltes an sich (BGH v. 23.09.2003 - VI ZR 335/02). In der Literatur stößt diese Auslegung auf unterschiedliche Meinungen. Die eine (Heckmann, 2007) sieht hier zu Recht ein Paradox, dass zusätzliche freiwillige (und wünschenswerte) Überwachung durch den Hostprovider zu einer Gefährdung seines Haftungsschutzes führen kann. Dies könnte für rationale Hostprovider einen Anreiz schaffen, den eingestellten Inhalten möglichst wenig Beachtung zu schenken. Die andere – unterstützende - Meinung (Spindler et al., 2004) warnt vor einer Aufweichung der positiven Kenntnis, da diese ausdrücklich vom Gesetzgeber vorgesehen sei.

Zusätzlich ergibt sich die Frage nach der Kenntnis der mit dem Inhalt verbundenen Rechtsverletzung. Von der E-Commerce Richtlinie (2000/31/EG) - der das Gesetz entsprechen soll - wird diese unbedingt gefordert damit der Haftungsschutz nicht greift (Art. 14, 1, a: „Kenntnis von der rechtswidrigen Tätigkeit ODER Information“). In den Fällen der Straftaten (2.2.1) offenbart das alleinige Kennen des Inhaltes auch dessen Rechtswidrigkeit. Zwar greifen auch hier Verbotsirrtum und Tatbestandsirrtum des

Strafrechts, grundsätzlich ist es jedoch jedem Hostprovider bekannt, wenn ein Inhalt gegen strafrechtliche Verbote verstößt. Interessanter ist die Frage jedoch, wenn sich die Rechtswidrigkeit eines Inhaltes nicht direkt aus dem Inhalt in Verbindung mit dem Gesetz, sondern aus Rechten Dritter ergibt (wie beispielsweise dem verbotenen Verwenden einer geschützten Marke). Damit das Haftungsprivileg des Hostproviders aus § 11 TMG entfällt, muss diesem - unter Betrachtung der E-Commerce Richtlinie - zusätzlich zum Inhalt, auch das Bestehen eines fremden (z. B. Marken- oder Urheber-) Rechtes bekannt sein (so auch Heckmann, 2007; Spindler et al., 2004).

Liegt im einen oder anderen Fall keine Kenntnis vor, ist der Hostprovider vor strafrechtlichen Konsequenzen und Schadensersatz geschützt. Jedoch hat der Bundesgerichtshof den Schutz des Hostproviders vor zivilrechtlichen Unterlassungsansprüchen verneint (BGH v. 11.03.2004 – I ZR 304/01). Zu begründen ist dies wiederum mit der E-Commerce Richtlinie. In Artikel 14 Absatz 3 wird klargestellt, dass das jeweilige inländische Gericht den Dienstanbieter dazu verurteilen kann, „die Rechtsverletzung abzustellen oder zu verhindern“. Diesem Unterlassungsanspruch steht der § 11 folglich auch dann nicht entgegen, wenn er sich auf in Zukunft zu befürchtende Störungen bezieht. Im Internet besteht eine ständige Wiederholungsgefahr, da der Hostprovider an derselben Verletzung mitwirken kann, auch wenn der eigentliche Täter ein anderer ist. Der Anspruchsgläubiger muss nicht abwarten, bis dieser Fall eintritt.

2.4. Zwischenergebnis: Inhaltsüberwachung als mögliche Folge

Im Internet existieren unzählige Möglichkeiten zu rechtswidrigem Verhalten, die nach Deutschem Recht geahndet werden können. Für den Hostprovider stellen die möglichen Konsequenzen des Fehlverhaltens seiner Nutzer ein unkalkulierbares Risiko dar. Aus diesem Grund existiert das Haftungsprivileg des Telemediengesetzes und kommt seinem Bedürfnis nach Rechtssicherheit nach, indem es ihn eindeutig vor strafrechtlichen Folgen und Schadensersatzforderungen schützt. Die Pflicht zur Löschung konkret angemahnter Inhalte (sog. „notice and take-down“-Verfahren) besteht jedoch zu Recht uneingeschränkt, da er Kenntnis vom Inhalt erhält.

Doch auch der zivilrechtliche Unterlassungsanspruch gegen Wiederholungstaten kann gegen den Hostprovider erfolgreich sein. Besonders in Bezug auf Urheber- oder Markenrecht ist er im Internet von großer Bedeutung. Er ergibt sich aus der

Störerstellung des Hostproviders und ist - nach der Rechtsprechung - nicht von den Schutzvorschriften des Telemediengesetzes gedeckt.

Aus diesem Anspruch für den Hostprovider ergibt sich faktisch eine Pflicht zur Überprüfung zukünftig eingestellter Inhalte, wenn er gegen ihn aufgrund einer vorgelagerten Rechtsverletzung geltend gemacht wurde. Geht man diesen Gedanken weiter, könnte der Hostprovider auch vorbeugend auf Unterlassung in Anspruch genommen werden, wenn eine unmittelbar drohende Erstbegehungsgefahr besteht. Dies könnte dazu führen, dass der Hostprovider alle eingehenden Inhalte auf eine Unzahl möglicher Rechtsverletzungen zu prüfen hat, um einer Haftung zu entgehen. Die Haftung bestünde namentlich für die gerichtlichen Zwangsmaßnahmen um den Unterlassungsanspruch durchzusetzen (Ordnungsgeld, Zwangsdurchsetzung etc.).

Weder dem Gesetzgeber noch der Rechtsprechung ist es jedoch bislang gelungen, die Art dieser Pflicht genau zu spezifizieren, was wiederum zu Rechtsunsicherheit führt. Der Abwägung der verletzten Rechte gegen das wirtschaftliche Interesse des Hostproviders kommt damit besondere Bedeutung zu.

3. Wirtschaftliche Implikationen

Dieser Abschnitt soll Klarheit über die konkurrierenden Interessen des Anspruchspetenten und -repetenten geben. Auf der einen Seite steht die Beeinträchtigung der Rechte, auf der anderen das wirtschaftliche Interesse des Hostproviders am Funktionieren seines Geschäftsmodells. Auch wenn im römischen Recht der Grundsatz „iudex non calculat“ gilt (lat. „Der Richter rechnet nicht“; greift eigentlich bei der Bemessung der Verfahrenskosten, hier jedoch übertragen.), ist eine wirtschaftliche Betrachtung der Interessen durchaus sinnvoll. Schließlich soll diese eine Basis für die in Teil 4 getroffene Abwägung bieten.

3.1. Beeinträchtigung der Rechte des Markeninhabers

Die Markierung von Gütern lässt sich auf die Frühgeschichte der Menschheit zurückdatieren, so wurden schon auf ägyptischen, griechischen und römischen Tonkrügen signalhafte Kennzeichnungen vorgenommen (Mattmüller/Thunder, 2004, S. 217). Die Marke erhebt ein Produkt aus der Anonymität (Mattmüller, 2004, S. 180) und birgt bestimmte Informationen für den Verbraucher. Dieser verbindet mit ihr eine

gewisse Vorstellung über Qualität, ungefähren Preis und Herkunft des Produktes. Die so gewonnene subjektive Information kann die Kaufentscheidung des Verbrauchers zuweilen stärker positiv oder negativ beeinflussen als manch objektive. Jedoch ist ein positives „Markenimage“ für den Markierenden in den seltensten Fällen ohne Aufwand zu erreichen, sondern dieser muss in irgendeiner Form in Vorleistung treten. Dieses geschieht durch besonders gute Erfahrung des Kunden bei vorherigen Transaktionen, durch Marketingaktivität oder durch das Einhalten bestimmter Verpflichtungen bei der Herstellung (beispielsweise „Bio“-Produkte). All dies ist für den Markierenden mit monetärem Aufwand verbunden und es ist legitim, dem aus der Marke entstehenden Wettbewerbsvorteil ebenso eine monetäre Größe zuzuordnen. Der Marke Coca-Cola wird so beispielsweise ein Wert von rund 50 Milliarden Euro beigemessen (Forbes, 2005). Auch wenn sich der deutsche Gesetzgeber noch gegen eine bilanzrechtliche Anerkennung selbst geschaffenen Markenwertes sträubt, ist diese nach internationalen Standards bereits möglich (siehe zur Bilanzierung von Marken: Nickel, 2006). Dass dieser Wert ein schützenswertes Gut ist, hat der Gesetzgeber bereits 1874 mit dem Warenzeichengesetz bestätigt und den Schutz 1995 durch das Markengesetz erweitert.

Wird eine Marke unerlaubt verwendet, stiehlt der Verwender dem rechtmäßigen Markenbesitzer sozusagen die Früchte aus dessen Investition in den Aufbau der Marke. Es muss die Frage gestellt werden, in welchen Größenordnungen sich dieser Diebstahl bewegt. Auf Grund der Aktualität und da dieser Streitfall bereits mehrfach Erwähnung gefunden hat, bietet es sich an, die Schädigung der Rolex AG durch den Verkauf gefälschter Uhren auf Ebay beispielhaft zu untersuchen:

Der Wert des Markennamen Rolex und die ihm zugehörigen Markenzeichen wird 2006 auf rund 5,849 Milliarden Schweizer Franken (3,2684 Milliarden Euro, Wechselkurs am 23.01.2008) geschätzt (Quelle: Interbrand Zintzmeyer & Lux, 2007). Dem steht ein verhältnismäßig geringer Umsatz von rund 82 Millionen Euro in Deutschland gegenüber (Quelle: Hoppenstedt, 2008). Wer unberechtigt eine mit „Rolex“ markierte Uhr in Deutschland in Verkehr bringt, macht sich also ein Vermögensgut von verhältnismäßig großem Wert zu nutze. Auf den einzelnen Fall bezogen ist dieser Wert die Differenz der Herstellungskosten der Firma Rolex zum Listenpreis unter Abzug der Marge, die gewöhnlich beim Verkauf einer nicht speziell markierten (in der Theorie, praktisch existiert kein nicht markiertes Produkt) Uhr erzielbar ist.

Doch ist dieser Wert (Gewinn) nicht vollständig als gestohlen (entgangen) anzusehen, wenn der Verbraucher höchstwahrscheinlich ohnehin niemals ein Produkt der Firma Rolex erworben hätte. In dem angesprochenen Streitfall kann es ausschließlich um solche Produkte gehen, welche für Ebay (und folglich auch für den Verbraucher) in irgendeiner Form bereits vor dem Kauf als Fälschungen zu erkennen sind (notwendige Erkennbarkeit für die Störerhaftung). Dies bedeutet, dass der Verkauf nur an solche Personen geschehen kann, die explizit an einer Fälschung interessiert sind. Es ist billig anzunehmen, dass diese Verbraucher Rolex nicht durch den Verkauf entgangen sind, sondern von vorneherein keine Zielgruppe des Unternehmens waren.

Nun könnte Rolex einwenden, dass der Verkauf von Fälschungen zu einer Schädigung des Markenimages führt, da plötzlich Menschen die Uhr tragen, die nicht die hinter Rolex stehende Idee verkörpern (Claims: „Die Großen der Welt.“, „Die Großen der Gegenwart tragen Rolex-Uhren.“, „The crown for every achievement.“). Gleichzeitig lässt sich jedoch feststellen, dass Rolex sich heute immer mehr - strategisch oder ungewollt - in eine Position begibt, in der das Tragen einer Rolex lediglich den monetären Wohlstand des Trägers zum Ausdruck bringen soll. In dieser Position ist die allgemeine Bekanntheit des Markennamens von größter Bedeutung, zu welcher nun mal auch Fälschungen beitragen. Es lässt sich nur schwer beantworten, inwiefern sich diese beiden Effekte aufheben. Zum einen darf man annehmen, dass ein potenzieller Käufer einer Rolex in den seltensten Fällen auf eine Fälschung zurückgreifen wird. Zum anderen könnte bei zu starker Überflutung des Marktes mit Fälschungen der Nutzen einer Rolex als Statussymbol leiden (und damit die Nachfrage zurückgehen).

Aus den genannten Gründen bietet sich bei der Bewertung der Auswirkungen der Rechtsbeeinträchtigung das aus dem Schadensersatzanspruch bekannte Verfahren des Verletzergewinns an. Schließlich wäre ein Verkauf der Ware ohne das Ausnutzen des Markennamens Rolex nur sehr schwer möglich gewesen. Der fehlende Rest zur Unmöglichkeit lässt sich im Hinblick auf den Ausgleich des eventuellen Imageverlustes billig hinnehmen.

3.2. Beeinträchtigung der Rechte des Urhebers

Der Sinn des Urheberrechts offenbart sich, wenn man den entsprechenden englischen Ausdruck „Copyright“ betrachtet. Tatsächlich hat es seinen Ursprung in der

Vereinfachung der Druckkunst durch Gutenberg im 15. Jahrhundert. Druckern wurden von der jeweiligen Obrigkeit Rechte zur Vervielfältigung zugesprochen. Vom 16ten – 18ten Jahrhunderts entwickelte es sich dann zu dem durch die Schöpfung entstehenden Recht des Autors an seinem Werk (prägend: Kant, „Von der Unrechtmäßigkeit des Büchernachdrucks“, 1785; setzt erstmals das Urheberrecht auf die Stufe eines Persönlichkeitsrechts). Nur durch Gutenbergs Innovation, die eine massenhafte, kostengünstige Kopie von Werken zuließ, entstand das Problemfeld überhaupt. Eine ähnliche Auswirkung kann man dem folgend auch dem digitalen Zeitalter beimessen: CD-Brenner, MP3-Player und Festplatten sind der Buchdruck von heute.

Von den Gegnern der Verteidigung von Urheberrechten im Internet wird gerne ein Thomas Jefferson zugeschriebener Ausspruch zitiert: „He who receives an idea from me, receives instruction himself without lessening mine; as he who lights his taper at mine receives light without darkening me.“ (Deutsch: „Wer eine Idee von mir empfängt, mehrt dadurch sein Wissen, ohne meines zu mindern, ebenso wie derjenige, der seine Kerze an meiner entzündet, dadurch Licht empfängt, ohne mich der Dunkelheit auszusetzen.“). Jedoch lässt sich diese Metapher nicht ohne weiteres anwenden, da eine Idee zweifelsohne an Wert verliert, wenn sie sich jeder Beliebige zu nutze machen kann. Der Schöpfer hat möglicherweise großen Aufwand betrieben, um seine Idee aus den Tiefen seines Geistes an das Licht der Welt zu befördern und wäre nun um die Früchte seiner Investition betrogen. Somit ist es nur legitim, diese Früchte vor „Diebstahl“ zu schützen. Doch wie schon bei der Markenverletzung stellt sich auch hier die Frage nach der Größenordnung diese „Diebstahls“. Beispielhaft soll hier das Hosting von geschützten Musikdateien analysiert werden.

Die Musikindustrie leidet nachweislich unter der Entwicklung der Raubkopie im Internet (siehe auch Liebowitz, 2004). Allerdings lässt sich hier - analog zur Markenverletzung - argumentieren, dass die Downloader der Musikindustrie nicht immer als Kunden entgangen sind. Es ist möglicherweise vielmehr eine Nachfrage entstanden, die ohne die freie Verfügbarkeit der Musikstücke erst gar nicht existiert hätte. Der Preis für ein Musikstück im Internet ist sehr gering (Raubkopien bei Ebay), beziehungsweise Null, wenn die Datei frei auf einem Server liegt. Nach simpelsten ökonomischen Gesetzen ist die Nachfrage bei einem solchen Preis sehr viel größer als beim Listenpreis einer CD oder kommerziellen MP3. Es stellt sich die Frage, ob eine Raubkopie nun tatsächlich als Substitution eines legalen Erwerbs heruntergeladen

wurde oder lediglich aus der „Es-ist-kostenlos-warum-nicht“-Motivation. Eine ausführliche Studie von Sandulli (2007) geht dieser Frage nach und entdeckt eine starke Heterogenität von Download- und CD-Kaufverhalten. Es existieren somit beide Arten der Motivation. Es müssen bei der Bewertung der Rechtsbeeinträchtigung also bestimmte Abstriche gemacht werden, da nicht jeder Download ein „Diebstahl“ (in dem oben genannten Sinne) ist. Manche Meinungen gehen sogar noch weiter und argumentieren, dass die Vorteile aus illegalen Downloads (durch die bessere Möglichkeit zur Abstimmung des Originalproduktes auf die Konsumentenwünsche und dadurch höheren erzielbaren Endpreis) den Verlust mehr als überkompensieren (Waelbroeck / Peitz, 2005). Sicherlich ist diese Annahme jedoch etwas zu gewagt und es gilt, einen Mittelweg zu finden.

Für die Bewertung der Rechtsbeeinträchtigung kann man nicht einfach den möglichen Verkaufswert des Werkes mit der Anzahl der illegalen Downloads multiplizieren, sondern kann nur einen Teilwert ansetzen, um den oben genannten Erwägungen Rechnung zu tragen. Je nach Werk und Verbreitungsweg kann dieser Teilwert unterschiedlich ausfallen. So sind die zugrunde liegenden Annahmen möglicherweise für raubkopierte Musikdateien und Bücher, die ohne Entgelt heruntergeladen werden, valider, während beispielsweise Filme, welche über Ebay verkauft werden, eher als Substitutionskäufe anzusehen sind.

3.3. Vermeidungskosten für den Hostprovider

Die Vermeidungskosten für den Hostprovider sind wohl die dringendste Frage, da die Rechtsprechung direkt hierauf abstellt. Es sind drei Problemfelder abzugrenzen: Zum Ersten die Beseitigung der konkreten Verletzungsfälle, auf die der Hostprovider von den Rechteinhabern aufmerksam gemacht wird. Zum Zweiten die Unterlassung von Wiederholungsfällen. Zum Dritten das Verhindern der Erstbegehung aus der vorbeugenden Unterlassung.

3.3.1. Löschung bestehender Inhalte

Das Geschäft des Hostproviders ist es, fremde Inhalte zu verwalten. Hierzu gehört auch, das einfache Auffinden dieser zu sichern und sie mit einer eindeutigen Adresse zu versehen. Die Argumentation, es sei einem Hostprovider nicht zumutbar, Inhalte zu entfernen, auf die er konkret hingewiesen wurde, ist in Anbetracht dieser Aufgaben

absurd. Ob die Verpflichtung zur Beseitigung einer Rechtsverletzung nun aus der Störer- oder Täterstellung begründet ist, tut weiterhin nichts zur Sache. Könnte ein Hostprovider konkrete Inhalte nicht schnell und kostengünstig auffinden, den Zugang zu ihnen sperren oder sie löschen, wäre es ihm unmöglich, seinem tagtäglichen operativen Geschäft nachzukommen. In der Praxis wird dem von Seiten der Hostprovider auch nicht widersprochen, sondern eher im Gegenteil, den Rechteinhabern (beziehungsweise der Exekutive bei Strafsachen) entgegengekommen. So hat Ebay beispielsweise bereits im Jahr 2002 das so genannte VeRI (Verifizierte Rechte Inhaber)-Programm ins Leben gerufen. Mit Teilnahme an diesem Programm können Rechteinhaber laut Ebay „schnell und unkompliziert auf rechtheverletzende Angebote hinweisen und deren Löschung verlangen“ (Ebay Webseite, 2008). Diesem Versprechen kommt Ebay nach Tenor der Wortmeldungen auf einer Rechtsanwaltsveranstaltung zum Thema (GRU, 2008) auch nach und leitet in den meisten Fällen umgehend eine Löschung ein. Allerdings behält sich Ebay vor, ausschließlich auf Hinweise zu reagieren, die direkt von einem Rechteinhaber (beziehungsweise des ihn vertretenden Rechtsanwaltes) zu reagieren. Außerdem verpflichtet sich der Melder mit Ausfüllen des Antragsformulars faktisch für eventuelle Rechtsfehler (und beispielsweise daraus erwachsenen Schadensersatzforderungen) zu haften (Ebay Webseite, 2008). Jedoch erscheint dies beides, in Anbetracht des Schutzinteresses vor zu zahlreichen Falschmeldungen, legitim.

Die Löschung von bestehenden Inhalten stellt für den Hostprovider eine zumutbare Verpflichtung dar. Hierüber besteht ein Konsens beider Seiten. Mit der Tatsache, dass sich dieser bereits in einer solch praktischen Lösung wie dem VeRI-Programm niedergeschlagen hat, ist belegt, dass diese Verpflichtung den Hostprovider nicht übermäßig belasten kann.

3.3.2. *Unterlassung von Wiederholungen*

Im Zusammenhang mit der Prüfungspflicht des Hostproviders zum Verhindern von Wiederholungen der Rechtsverletzungen kommt erstmals der Begriff der technischen Maßnahmen ins Spiel. Jedoch wird auch eine manuelle Prüfung als Folgeschritt nicht ausgeschlossen. Auch hier lässt sich wieder Bezug nehmen auf die Aufgaben, mit denen ein Hostprovider im alltäglichen operativen Geschäft konfrontiert ist.

Bei den technischen Möglichkeiten ist eine Unterscheidung zwischen verschiedenen Gruppen von Hostprovider zu treffen. So gibt es Hostprovider bei denen der Nutzer lediglich einen so genannten FTP (File Transfer Protokoll) Zugang erhält. Die Inhalte werden direkt 1:1 auf den Server des Hostproviders übertragen, ohne dass sie auf dessen Seite ein spezielles Verarbeitungsprogramm durchlaufen. Dies sind die klassischen Webspacerprovider der Vor-web2.0-Generation (beispielsweise Serverflex, 1&1, Strato). In die zweite Gruppe fallen jene Hostprovider, bei denen Inhalte über eine Maske eingegeben und die Informationen kategorisiert in einer Datenbank abgelegt werden, um sie später aus dieser auszulesen und aufbereitet wiederzugeben. Diese stellen die neue Generation der Hostprovider dar; Myvideo.de, Myspace.com und Ebay.de fallen hierunter. Das Wesen des technischen Systems der ersten Gruppe von Host Providern liegt darin, Dateien aufzunehmen und auf den Server zu schreiben. Die Grundlagen hierzu sind durch die standardisierten Vorgänge des File Transfer Protocols (FTP) gegeben. Würde hier gefordert, den Inhalt der eingehenden Dateien durch ein weiteres Programm zu schicken, um beispielsweise nach einer bestimmten Zeichenfolge zu suchen, würde dies einen immensen Programmier-, sowie Rechenaufwand darstellen. In der zweiten Gruppe ist dies nun sehr viel leichter möglich, da das technische Wesen des Systems von Grund auf darauf ausgelegt ist, die eingehenden Informationen in vielfältiger Weise auszulesen. So muss eingehender Text schon aus dem Schutz vor Hackerangriffen ohnehin auf bestimmte Zeichenfolgen überprüft werden, da sich hinter einer scheinbar harmlosen Namenseingabe ein Script-Code verbergen könnte, der möglicherweise die Rahmenseite des Hostproviders gefährdet. Weiterhin werden die Eingaben der Nutzer analysiert und indiziert, um sie in der Seiteninternen Suchmaschine auffindbar zu machen. All dies impliziert bereits gewaltige Programmabläufe und Rechenanforderungen. Eine simple Erweiterung des Systems um eine weitere Überprüfung ist somit sehr viel einfacher durchzuführen als bei Host Providern der ersten Gruppe.

Ein weiterer Unterschied ergibt sich aus dem Typ von Information, welche durchsucht werden müssen. Den Inhalt von Multimediadateien (Bilder, Filme, Musik) zu durchsuchen ist technisch wesentlich aufwendiger als pure Textstrings zu vergleichen. Nicht umsonst werden im so genannten CAPTCHA-Verfahren („Completely Automated Public Turing test to tell Computers and Humans Apart“, engl. „Vollautomatischer öffentlicher Turing-Test, um Computer und Menschen zu

unterscheiden“) Bilddateien verwendet. Einem Computersystem ist es hier unmöglich, die Informationen aus dem Bild herauszulesen, was für einen Menschen kein Problem darstellt. Im Rahmen der Möglichkeiten, aber dennoch mit großem Rechenaufwand verbunden ist wohl einzig das Entdecken von zwei absolut identischen Bildern oder Videos (beispielsweise das von Youtube geplante Hashing-Verfahren, Spiegel Online, 2007) oder das Entdecken eines Markenzeichens in einem Computerbild mit einfarbigem Hintergrund.

Für den bereits in den vorherigen Teilen erwähnten Ebay-Fall lässt sich also folgendes festhalten. Ebay als Hostprovider der zweiten Gruppe, ist es nur bedingt technisch möglich, eingehende Angebote auf die Kriterien eines vorangegangenen Falls zu untersuchen, solange lediglich Texte nach bestimmten Kombinationen durchsucht werden (Beispielsweise „Rolex“+„Replika“ unter dem Ausnahmefall von „kein“ vor „Replika“) und im strengsten Fall identische Bilder gesucht werden müssen. Jedoch ist eine manuelle Nachkontrolle unerlässlich, da selbst die beste Suchsoftware hier Falschtreffer liefert. Nun liefert eine Suche nach „Rolex“ ca. 800 Treffer. Wird „Replika“, „Plagiat“ oder ähnliches hinzugefügt, liefert die Suche kein einziges Ergebnis mehr zurück (28.01.2008). Kriterien wie den Angebotspreis in die automatische Suche einzubeziehen, ist unter der legitimen Betrachtung, dass dieser nichts über den Endpreis der Auktion aussagt, nicht möglich (Ausnahme: Direktkauf). Könnte sich Ebay nun mit den null Treffern der „Replika“-Suche zufriedengeben, wäre dies auch im wirtschaftlichen Rahmen. Müssten jedoch die 800 Ergebnisse der „Rolex“-Suche im Folgeschritt manuell überprüft werden, wäre der Lohnaufwand hierfür immens.

3.3.3. *Verhinderung von Erstbegehung*

Die Verhinderung von erstmaligem Einstellen rechtsverletzender Inhalte, stellt einen Unterschied zu der Prüfung auf Wiederholungsfälle dar. Die Menge der Such- und Kontrollvorgänge würde gewaltig steigen. Der notwendige Personalaufwand, sich aus eigenem Antrieb mögliche Rechtsverletzungen auszudenken und eine Datenbank mit entsprechenden Suchmustern zu pflegen, kann wirtschaftlich nicht tragbar sein. Jeder Rechteinhaber würde zudem die Gelegenheit nutzen und sicherheitshalber ein Suchprofil einreichen und eine vorbeugende Unterlassung fordern.

3.3.4. Sonderfall: Handeln im geschäftlichen Verkehr

Zu erkennen, ob ein Nutzer eine Handlung im geschäftlichen Verkehr begeht, welches je nach Anspruchsgrundlage Voraussetzung sein kann, stellt ein (in Bezug auf Löschung, Vermeidung und Vorbeugung) übergreifendes Problem dar. Sich hier auf die wahrheitsgemäße Registrierung des Nutzers zu verlassen, wäre zwar angenehm, ist aber sicherlich nicht ausreichend. Gerade die Nutzer, die vorsätzlich rechtswidrig handeln, werden das Möglichste tun, ihren geschäftsmäßigen Hintergrund zu verschleiern. Dies geschieht beispielsweise durch das Anlegen einer Vielzahl von Nutzerkonten. Eine automatisierte Bündelung von Nutzeraccounts in einer natürlichen Person (Metanutzer; beispielsweise anhand von Werten wie Kontodaten oder Adressen) sollte für den Hostprovider noch durchführbar sein, da er daran auch für sein operatives Geschäft Interesse haben kann. Wurde ein rechtswidriges Handeln durch die zuvor genannten Suchverfahren eindeutig identifiziert, müssten diese Fälle dem Metanutzer zugeordnet und gespeichert werden. Ein so genanntes „Log“ (Aufzeichnung der Vorgänge auf der Plattform des Hostproviders) zu führen, gehört ebenso zu den Standardaufgaben des Hostproviders. Häufen sich in diesem Log die Verletzungsfälle, ist von geschäftsmäßigem Handeln auszugehen. Aber wie bereits gesagt, setzt all dies das Funktionieren der vorherigen Identifizierung der Rechtsverletzungen voraus. Dort liegt nun allerdings - wie gesehen - das eigentliche Problem.

3.4. Zwischenergebnis: Schaden und Vermeidungskosten

Die im Internet verletzten Schutzrechte sind in jedem Fall schutzwürdig, und es lässt sich den Beeinträchtigungen ein monetärer Wert zurechnen. Da das Durchsuchen von Inhalten für zumindest eine Gruppe von Host Providern zum notwendigen Tagesgeschäft gehört, sind die technischen Voraussetzungen gegeben, mindestens eine Textsuche durchzuführen. Einzig kritisch wird die Frage nach der Notwendigkeit von Personaleinsatz zur Nachprüfung, da dies einen zusätzlichen, für den normalen Geschäftsbetrieb nicht benötigten Aufwand darstellt. Genauso ist die vorbeugende Prüfung (ohne vorherigen Fall) höchstens noch dann wirtschaftlich tragbar, wenn die Rechteinhaber dem Hostprovider alle benötigten Informationen zukommen lassen und sich diese direkt für die Eingabe in das Suchsystem eignen. Abschließend lässt sich noch sagen, dass es bei Host Providern der zweiten Klasse (Ebay, myvideo, etc.) jedenfalls nur mit geringem Aufwand verbunden wäre, die Rechteinhaber automatisch

über Inhalte zu informieren, welche deren Markennamen oder Titel eines Werkes enthalten.

4. Abwägung

Die Prüfungspflicht nach allgemeinen Haftungsregeln (Verkehrspflichten) lässt sich verallgemeinern auf eine „Abwägung zwischen Aufwand für die Kontrollen, Verursachungsbeitrag zur Gefahr, Beherrschbarkeit der Gefahr und Sozialüblichkeit des Verhaltens“ (Spindler, 2001, S. 714). Diese vier Grundpfeiler muss man auch für die Störerstellung gelten lassen, um den Kreis der Passivlegitimierten nicht zu weit zu ziehen (siehe Haftung als Störer 2.3.2). In diesem Teil wird diese Abwägung nun vorgenommen. Sie führt zu einem praktisch anwendbaren Katalog der im Einzelfall zu überprüfenden Faktoren.

4.1. Generelle Zumutbarkeit

Der Hostprovider wird nie die wirtschaftliche Möglichkeit besitzen, eine rechtswidrige Handlung vollständig zu verhindern, ohne damit sein Überleben maßgeblich zu gefährden. Genauso wenig wie die Polizei die Möglichkeit besitzt, sämtliche Straftaten aufzudecken. Ab einem bestimmten Punkt überschreitet der Grenznutzen (durch Vermeidung der Beeinträchtigungen 3.1, 3.2) nun einmal die Grenzvermeidungskosten (3.3) und das Optimum wird verlassen. In der Störerstellung ist die Haftung des Hostproviders aus diesem Grund bereits auf der Tatbestandsseite eingeschränkt (Volkman, 2005, S. 123). Der Störer darf nur durch eine Haftung (aus Missachtung der Unterlassung) für solche Rechtsbeeinträchtigungen gefährdet sein, die er im wirtschaftlich sinnvollen Rahmen erkennen und abstellen kann.

Es lassen sich jedoch auch geradezu hetzerische Meinungen finden, die jegliche wirtschaftlichen Argumente der Abwehr zurückweisen. So schrieb Lehment (2003, S. 1060) ausdrücklich - Ebay wird hier in der Täterstellung gesehen: „Erklärt ein Anbieter, wirtschaftlich zur Kontrolle des Marktplatzes nicht in der Lage zu sein, so muss dieser notfalls geschlossen werden.“ Dies läuft natürlich den Grundsätzen des Eigentumsrechtes entgegen, ließe es sich doch sinngemäß auf allerlei Bereiche übertragen. So kann beispielsweise ein Betreiber eines tatsächlichen physikalischen Marktplatzes nicht hundertprozentig garantieren, dass nicht an dem einen oder anderen

Stand Alkohol an Jugendliche ausgeschenkt oder unter der Hand gestohlene Waren verkauft werden. Niemand würde hier auf die Idee kommen, eine Schließung des Marktes zu verlangen, wenn der Betreiber wenigstens hin und wieder Kontrollgänge veranlasst. Niemand würde weiterhin verlangen, dass er über seine wirtschaftliche Tragfähigkeit Personal einstellt, um solche Kontrollgänge durchzuführen, was schließlich auch zur Einstellung des Marktplatzes führen würde.

Diese Meinung ändert sich auch nicht dadurch, dass der Betreiber unglücklicherweise über die einheitlichen Standgebühren von dem rechtswidrigen Handeln profitiert. Dieses Beteiligungs-Argument wird gerne, beispielsweise gegen Ebay, verwendet. Dem Grunde nach trifft es zu, es wäre jedoch zu vermessen Ebay, mit einem in Deutschland erzielten Jahresumsatz von 600 Millionen Euro (Quelle: Hoppenstedt), zu unterstellen, es hätte besonderes wirtschaftliches Interesse an rechtswidrigem Handel. Es gibt hier eindeutig Unterschiede zwischen den Host Providern. Es muss im Zweifelsfall festgestellt werden, ob ein Hostprovider rechtswidriges Handeln aus wirtschaftlicher (oder ideologischer) Motivation fördert (Beispiel: <http://www.thepiratebay.org/>), nur ungewollt von rechtswidrigen Transaktionen profitiert (wie Ebay) oder sich möglicherweise in einer Grauzone befindet. Die Einstellung des Hostproviders nachzuweisen dürfte kein großes Probleme darstellen. Gibt es zahlreiche Hinweise und ernstzunehmende (also mit Sanktionen belegte) Warnungen des Hostproviders vor rechtswidrigem Handeln gegenüber dessen Nutzern, kann davon ausgegangen werden, dass dieser kein Interesse an Rechtsverletzungen seiner Nutzer hegt. Lässt sich nachweisen, dass ein Hostprovider rechtswidriges Verhalten bewusst die Augen verschließt, so ist dies als Unterstützung zu werten und gegen ihn zu verwenden (analog § 826 BGB; Spindler 2001, S. 739).

Weiterhin werden auch die technischen Möglichkeiten der Hostprovider überschätzt. Das „Erkennen identischer Datensätze“ (Lehment, 2003, S. 1060) ist, wie im vorherigen Teil (3.3) dargelegt, in bestimmten Fällen sehr einfach, jedoch stellt schon die geringste Änderung - und sei es ein Rechtschreibfehler - das System vor enorme Anforderungen. Gleiches gilt - für diese Meinung - in Bezug auf Multimediadateien. Weiterhin ist das Argument, die Anzahl der Falschergebnisse bei einer Weiterfassung der Suche wären so gering, dass eine menschliche manuelle Nachkontrolle durchaus zumutbar wäre, generell nur schwer glaublich (3.3.2: „Rolex“ + „Replika“); kann dies doch von Einzelfall zu Einzelfall extrem unterschiedlich ausfallen.

4.2. Verbot der totalen Inhaltsüberwachung

Trotz der legitimen Ausnahme des Unterlassungsanspruchs aus dem Schutz des Telemediengesetzes (2.3.3), darf dies nicht dazu führen, dass der Hostprovider in eine generelle Pflicht zur Inhaltsüberwachung gedrängt wird.

Übergeordnet würde eine generelle Vorab-„Zensur“ dem Interesse der Allgemeinheit an Meinungs- und Pressefreiheit (manifestiert in § 5 Grundgesetz) entgegenlaufen. Sie könnte dazu führen, dass legale Inhalte von der Veröffentlichung im Internet ausgeschlossen werden, da sie fälschlicherweise als illegal klassifiziert und abgewiesen wurden.

Spezieller könnte eine generelle Überwachungspflicht auch nicht ausdrücklicher verboten sein, als es in § 7 Abs. 2 Telemediengesetz, beziehungsweise Artikel 15 der E-Commerce Richtlinie geschieht. Die Verwendung der Begriffe „Entfernung und Sperrung“ in § 7 macht deutlich, dass es nur um - in irgendeiner Form - bereits bekannte Inhalte gehen kann. Eine Ausweitung der Unterlassung auf eine Erstbegehungsgefahr ist schon gesetzlich nicht möglich (nunmehr entgegen der Rechtsprechung BGH v. 19.04.2007 – I ZR 35/04; unterstützend: Leible / Sosnitza, 2007; nach diesen Sobola / Kohl, 2005), zudem wirtschaftlich und technisch nicht zumutbar (4.3), unabhängig des Wertes, den das verletzte Rechtsgut (3.1 + 3.2) einnimmt.

Ohne dieses Verbot würde der Hostprovider nicht existieren und seine nutzbringende Funktion ausfüllen. Diese Funktion ist namentlich die „Erbringung grundlegender Dienste [...], die den kontinuierlichen freien Informationsfluss im Netz gewährleisten“ (KOM, 2003, S.14). Vollständige Kontrolle würde eine ineffiziente Abwälzung von Aufwand aus einer Transaktion Dritter auf den Hostprovider bedeuten. In der Volkswirtschaftslehre, genauer der Neuen Institutionen Ökonomie, existiert hierfür der Begriff der „externen Effekte“. Wäre die vollständige Kontrolle Pflicht, könnte „Hostproviding“ nicht mehr über den Markt geschehen, sondern müsste hoheitlich zur Verfügung gestellt werden.

4.3. Stellenwert des Rechtsschutzes gegenüber modernen Geschäftsmodellen

Es sollte möglich sein, die Aktivität des Hostproviders im Rahmen des sozialüblichen Verhaltens zu bewerten. Je nach Wertigkeit des Rechtsgutes kann ein ausreichendes oder mangelhaftes Entgegenkommen festgestellt werden. Den gewerblichen

Schutzrechten lässt sich eine eindeutige wirtschaftliche, monetäre Bedeutung zuordnen. Dem kann der Hostprovider ein wirtschaftliches Interesse am Funktionieren seines Geschäftsmodells auf gleicher Ebene entgegenhalten. So muss man bei Verletzung von Marken- oder Urheberrechten in Störerstellung folglich auch einen stärkeren Verweis auf wirtschaftliche Belastung des Hostproviders zur Abwehr zulassen.

Genauso ineffizient wie eine totale Überwachungspflicht des Hostproviders (4.2) ist es jedoch vollständig und einzig den Verletzten die Pflicht zum Auffinden von Beeinträchtigungen ihrer Rechte aufzuerlegen, da sie noch mit weitaus schlechteren Möglichkeiten hierzu ausgestattet sind. Diese Ineffizienz wird bereits dadurch belegt, dass das Spannungsfeld ausreichend Nährboden für Unternehmen bietet, die sich auf das Auffinden von Rechtsverletzungen, beispielsweise Markenpiraterie, im Internet spezialisiert haben (S&I, 2006). Es gilt also ein Optimum zu finden auf das beide Seiten entsprechend der ökonomischen Effizienzkriterien hinarbeiten haben.

An dieser Stelle ist noch anzumerken, dass die Interessen nicht immer konträr sein müssen. So haben natürlich gerade gewerbliche Schutzrechtsinhaber auch Interesse an einem Funktionieren des Internets aus infrastruktureller Sicht. Je mehr Hostprovider erfolgreich wirtschaften können, umso besser werden die Möglichkeiten für Urheber- oder Markeninhaber ihre Produkte oder Werke über die neu entstandenen Vertriebswege abzusetzen.

4.4. Zwischenergebnis: Sinnvolle Prüfung

Der Begriff der technischen Möglichkeit ist in der Abwägung überflüssig, da eng an die wirtschaftliche Zumutbarkeit geknüpft. Eine wirtschaftlich mögliche Handlung muss zwingend technisch möglich sein. Eine technisch unmögliche Handlung ist genauso zwingend auch wirtschaftlich unmöglich. Kombiniert man beide, die wirtschaftliche UND technische Zumutbarkeitsbedingung, kann man sich lediglich mit der Prüfung der wirtschaftlichen begnügen.

Eine absolute, allgemeingültige Wertung der Zumutbarkeit ist - wie gesehen - unmöglich und auch vom Gesetzgeber nicht gewünscht. Darum gibt es Meinungen (s. o. Leible), die den Hostprovider aus dem Rechtssicherheitsinteresse komplett von einer Prüfung freistellen wollen. Diese lässt sich jedoch aus Sicht der Effizienz ebenso wenig

wie die absolute Kontrollpflicht unterstützen. Es muss also im Einzelfall eine Wertung nach folgenden Faktoren geschehen:

- 1) Wird ein Rechtsgut von großem Wert beeinträchtigt, so kann dem Hostprovider auch größerer wirtschaftlicher Aufwand abverlangt werden. Zieht der Hostprovider zusätzlich bewusst und offenkundig Vorteile aus dem rechtswidrigen Verhalten, muss dies ebenfalls angerechnet werden.
- 2) Je größer das allgemeine Interesse an der Dienstleistung, welche der Hostprovider zur Verfügung stellt, umso geringer sollte die Belastung des Hostproviders sein, um dessen Existenz zu garantieren.
- 3) Je besser die Möglichkeiten der Verletzten zur Prüfung sind, umso geringer sollte der Anteil des Hostproviders sein.

Kommt der Hostprovider seinen Pflichten aus diesem Rahmen nach, ist er unschuldig und muss keine Haftung (für eventuelle Zwangsmaßnahmen) aus der Nichtbeachtung von Unterlassungspflichten gegen sich gelten lassen. Hiermit wäre der Hostprovider vor unverhältnismäßiger Gefährdung geschützt, aber der Anreiz, die Augen nicht vor Rechtsverletzungen zu verschließen, dennoch gewahrt.

5. Fazit und Ausblick

Die „Unterhöhlung“ des Hostproviderschutzes durch die Rechtsprechung lässt sich nachvollziehen und die daraus entstandene Diskussion als nützlich einstufen. Um den schmalen Grad zwischen Nutzen und Gefahren des Internets zu finden, ist das klassische Bild des Täters nicht ausreichend. Der Hostprovider darf weder als Mittäter verdammt noch als Unbeteiligter komplett freigestellt werden. Vielmehr muss er als Vermittler agieren. Seine Freiheit und Existenz muss geschützt werden, allerdings verpflichtet seine Position auch zum Wohlverhalten:

Ein beispielhafter Hostprovider greift unverzüglich nach Bekanntwerden einer Rechtsverletzung ein und entfernt diese. Er kommt den Verletzten hier entgegen, indem er die Meldung von Rechtsverletzungen so einfach wie möglich gestaltet. Zudem implementiert er Erweiterungen in den bereits vorhandenen Suchsystemen, in die sich die eindeutigen Schlüsselkriterien der vorangegangenen Rechtsverletzung, soweit sie

sich eignen, eintragen werden. Ist sein Angebot überwiegend von zweifelhaftem allgemeinem Nutzen und bietet erhöhtes Gefahrenpotenzial (beispielsweise Pornographie), betreibt er weiteren Aufwand und führt manuelle Stichproben durch. Überdies richtet er ein Meldesystem ein, das Rechteinhaber über potenziell verletzende Inhalte informiert (da sie beispielsweise deren Markennamen enthalten) und reduziert so deren Suchaufwand.

Unter der Betrachtung, dass eine Vorab-„Zensur“ der Inhalte weder möglich, noch wünschenswert ist, muss dies die Maximalanforderung darstellen. Dieser Hostprovider hat seine Prüfungsmöglichkeiten in jedem Fall im zumutbaren Rahmen ausgeschöpft und kann sich nicht vorwerfen lassen, er hätte Prüfungspflichten verletzt. Er ist also nicht schuldig.

Um dem praktischen Bedürfnis der Rechtssicherheit Rechnung zu tragen, wäre es denkbar, eine unabhängige, privatrechtliche Zertifizierungsstelle einzurichten, die dem Hostprovider jeweils diese - in jedem Fall - ausreichende Prüfungsvorkehrungen attestiert. Vor Gericht müsste der Hostprovider dann gegebenenfalls auf dieses Testat verweisen und sich sicher auf dessen Abwehrwirkung verlassen können. Die Zertifizierungsstelle könnte nach dem Vorbild bestehender Qualitätssicherungsorganisationen entwickelt werden. Jedenfalls würde das Bestehen eines solchen Testats einen endgültigen Schlussstrich unter die Diskussion der Prüfungspflichten und Prüfungsmöglichkeiten setzen. Die theoretische Ausgestaltung einer solchen Zertifizierung könnte ein geeignetes Thema weiterer Forschung auf diesem Gebiet sein.

Literatur

Normen:

E-Commerce Richtlinie vom 08.06.2000 (2000/31/EG)

BT-Drucksache 14/6098 - Gesetzesentwurf zum Teledienstgesetz

Bürgerliches Gesetzbuch (BGB) v. 18.08.1896 - letzte Änderung in Kraft am 01.01.08

Jugendschutzgesetz (JuSchG) v. 23.06.2002 - letzte Änderung in Kraft am 01.09.07

Gesetz gegen den unlauteren Wettbewerb (UWG) v. 07.06.1909 – letzte Änderung in Kraft am 29.12.06

Markengesetz (MarkG) v. 25.10.1994 – letzte Änderung in Kraft am 01.01.07

Strafgesetzbuch (StGB) v. 15.05.1871 – letzte Änderung in Kraft am 01.01.08

Telemediengesetz (TMG) v. 26.02.2007 – in Kraft getreten am 01.03.07

Teledienstgesetz (TDG) a. F. v. 22.07.1997 – außer Kraft am 01.03.07, durch TMG

Urheberrechtsgesetz (UrhG) v. 09.09.1965 – letzte Änderung in Kraft am 01.01.08

Urteile:

OLG Köln v. 18.03.2005 - 6 U 12/01: "Rolex" - Versteigerung von Plagiaten

BGH v. 13.10.2004 - I ZR 163/02: Hotel Maritim

OLG Bremen v. 17.02.2000 - 2 U 139/99: Gerichtsstand für Wettbewerbsverstöße im Internet

BGH v. 19.10.2007 - I ZR 102/05: Altersverifikation im Internet

BGH v. 12.07.2007 - I ZR 18/04: Jugendgefährdende Medien bei eBay

LG Berlin v. 9.11.2001 - 103 O 149/01: Geschäftsmäßiges Handeln im Internet

AG Brakel v. 11.02.1998 - 7 C 748/97: Unverlangte E-Mail-Werbung

BGH v. 19.04.2007 – I ZR 35/04: Internet-Versteigerung II

BGH v. 10.10.1996 - I ZR 129/94: Architektenkammer

BGH v. 17.05.2001 – I ZR 251/99: ambiente.de

BGH v. 11.03.2004 – I ZR 304/01: Internet-Versteigerung I

BGH v. 23.09.2003 - VI ZR 335/02: Haftung des fremde Inhalte anbietenden Internetproviders

Schrifttum:

Balestrino, Alessandro (2007). *It is a theft but not a crime* in European Journal of Political Economy *im Druck*

Burden, Kit / Palmer, Creole (2003). *Internet crime: Cyber Crime — A new breed of criminal?* in Computer Law & Security Report, V. 19, Nr. 3. S. 222-227

Devezas, Tessaleno C. / Linstone, Harold A. / Santos Humberto J.S. (2005). *The growth dynamics of the Internet and the long wave theory* in Technological Forecasting & Social Change V. 72, S. 913–935

Gottschalk, Silke / Kröger, Detlef (Hrsg.) (2002). *Vertragsgestaltung bei Content und Access Providern* in *Handbuch zum Internetrecht*. Springer, Berlin [u.a]

Heckmann, Dirk (2007). *Internetrecht*. Juris, Berlin

Jäger, Marc (2007). *Das neue Telemediengesetz (Teil 1) – Grundlagen* Juris Praxisreport IT-Recht 4/2007 Anm. 4

Jugendschutz.net – Schindler, Friedemann (2007). *10 Jahre Jugendschutz im Internet*. Festschrift. <http://www.jugendschutz.net/pdf/festschrift.pdf> (abgerufen am 16.01.2007)

Kant, Immanuel (1785). *Von der Unrechtmäßigkeit des Büchernachdrucks* in Berlinische Monatsschrift, 05/1785, S. 403-417

KOM – Kommission der Europäischen Gemeinschaften (2003). *Bericht der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss*. KOM(2003) 702 endgültig.

Lehment, Cornelius (2003). *Zur Störerhaftung von Online-Auktionshäusern* in Wettbewerb in Recht und Praxis 2003, S. 1058-1065

Leible, Stefan / Sosnitza, Olaf (2007). *Haftung von Internetauktionshäusern – reloaded* in Neue Juristische Wochenschrift 46/2007, S. 3324-3326.

Liebowitz, Stan J. (2004). *Will mp3 downloads annihilate the record industry? The evidence so far* in Advances in the Study of Entrepreneurship, Innovation, & Economic Growth, 15/2004, S. 229-260

Mattmüller, Roland (2004) *Integrativ Prozessuales Marketing*. Gabler, Wiesbaden.

Mattmüller, Roland / Thunder, Ralph (2004) *Strategisches Handelsmarketing*. Vahlen, München

Nickel, Rüdiger-Waldemar (2006). *Der Markenwert Ermittlung – Bilanzierung – Auswirkungen von IFRS* in Wismarer Diskussionspapiere. http://www.wi.hs-wismar.de/~wdp/2006/0605_Nickel.pdf (abgerufen am 23.01.2008)

OVG - Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V. (2007) - *Jahresbericht 2006*. <http://www.gvu-online.de/media/pdf/249.pdf> (abgerufen am 17.01.2008)

Peitz, Martin / Waelbroeck, Patrick (2005). *Why the music industry may gain from free downloading — The role of sampling* in International Journal of Industrial Organization, 24/2006, S. 907-913

S&I, Tobias Knopp (2006). *Markenpiraten auf der Spur* in Sicherheit & Industrie 11/2006, S. 49-51

Säcker, Christopher (2001). *Die Haftung von Diensteanbietern nach dem Entwurf des EGG* in Multimedia und Recht 9/2001, S. 2-4

Sandulli, Francesco D. (2007) *CD music purchase behaviour of P2P users* in Technovation, 27/2007, S. 325-334

Seyfert, Christian (2006). *Sekundärhaftungsrisiko für Anbieter von BitTorrent-Anwendungen in den USA und in Deutschland* in MIR 2006, Dok. 084, Rz. 1-12 http://medien-internet-und-recht.de/volltext.php?mir_dok_id=299 (abgerufen am 17.01.2008)

Sobola, Sabine / Kohl, Kathrin (2005). *Haftung von Providern für fremde Inhalte - Haftungsprivilegierung nach § 11 TDG - Grundsatzanalyse und Tendenzen der Rechtsprechung* in Computer und Recht 6/2005, S. 443-449.

Solmecke, Christian (2006). *Filesharing - Straf- und zivilrechtliche Konsequenzen* in Multimedia und Recht 7/2006, S. 23-24

Spindler, Gerald (2001). *Die Zivilrechtliche Verantwortlichkeit von Internetauktionshäusern – Haftung für automatisch registrierte und publizierte Inhalte?* in Multimedia und Recht 11/2001, S. 737-743

Spindler, Gerald (2002). *Das Gesetz zum elektronischen Geschäftsverkehr - Verantwortlichkeit der Diensteanbieter und Herkunftslandprinzip* in Neue Juristische Wochenschrift 13/2002, S. 921-922

Spindler, Gerald / Schmitz, Peter / Geis, Ivo (2004). *TDG: Teledienstegesetz, Teledienstdatenschutzgesetz, Signaturgesetz ; Kommentar*. Beck, München.

Stadler, Thomas (2005). *Haftung für Informationen im Internet*. E. Schmidt, Berlin

Taeger, Jürgen / Wiebe, Andreas (Hrsg.) (2006). *Aktuelle Rechtsfragen von IT und Internet* Oldenburger, Edewecht

Volkman, Christian (2005). *Der Störer im Internet*. Beck, München.

Wenning, Rigo (1998). *Akteure im Internet: rechtliche Problemfeld* JurPC Web-Dok. 46/1998. <http://www.jurpc.de/aufsatz/19980046.htm> (abgerufen am 15.01.2007)

Wurster, Bettina (2001). *Persönlichkeitsrechtsverletzungen im Internet*. JurPC Web-Dok. 249/2000. <http://www.jurpc.de/aufsatz/20010249.htm> (abgerufen am 16.01.2007)

Sonstige:

Alexa.com - The Web Information Company. *Liste der meistbesuchten Webseiten* http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none (abgerufen am 15.01.2008)

Jupiter Research (2006) in GMID - Global Market Information Database: *Online shopping expenditure: Germany*. Euromonitor International (abgerufen am 16.01.2007)

Interbrand Zintzmeyer & Lux (2007). *The 50 most valuable Swiss Brands*. Pressemitteilung v. 18.01.2007. http://www.ourfishbowl.com/images/surveys/2006_CH_Marken_PressRelease_e.pdf (abgerufen am 23.01.2008)

Hoppenstedt Firmeninformationen GmbH, Darmstadt (2008) *Umsatzinformationen ebay Deutschland GmbH*

Ebay Deutschland (2008). *Das Verifizierte Rechteinhaber-Programm (VeRI)*. <http://pages.ebay.de/vero/about.html> (abgerufen am 28.01.2008)

Populärmedien:

Kump, Lesley / Badenhausen, Kurt / Roney, Maya (2005). *Beyond The Balance Sheet: Brand Value*. in Forbes Online, 06.02.05

„lis“ (2007). *Arcor blockiert Zugang zu Youporn* in Spiegel Online, 23.10.2007

„lis“ (2007). *Myspace schlägt Pornos* in Spiegel Online, 23.04.2007

OV (2007) *Jungliberale: Pornos für Jugendliche erlauben* in Süddeutsche Zeitung, 14.02.2007

Pörtner, Rainer / Wiegold, Thomas (2007). *Dr. Jekyll & Mr. Hyde am PC* in Focus Magazin, 12.02.2007

„AP/cor“ (2007). *Besserer Schutz Minderjähriger vor Internet-Pornografie* in Welt Online, 19.10.2007

Patalong, Frank / Lischka, Konrad (2007). *Google bastelt den Super-Filter* in Spiegel Online, 30.08.2007

Anhang: Fallstudien

Anhand der folgenden praktischen Beispielfälle sollen Ergebnisse der Arbeit noch einmal verdeutlicht und überprüft werden. Die hier dargestellten Fälle sind rein fiktiv. Es wurde ein Fall aus dem Strafrecht und einer aus dem Bereich des Urheberrechts gewählt.

Volksverhetzung auf wikipedia.de

Sachverhalt:

Internetnutzer X hat sich beim Dienstanbieter wikipedia.de unter Angabe eines kryptischen Nutzernamens und temporärer Emailadresse angemeldet. Er verändert den Artikel „Holocaust“ dahingehend, dass er einen Absatz hinzufügt, in dem die Existenz von Konzentrationslagern geleugnet wird. Dieser Absatz enthält weiterhin drastische Beleidigungen und Beschimpfungen gegen die im Dritten Reich verfolgten Minderheiten. Ein anderer Nutzer X2 versucht mehrfach, diese Aussagen zu entfernen, bleibt aber erfolglos, da X ihn hartnäckig wieder einfügt. X2 informiert daraufhin Wikipedia per E-Mail über den Inhalt. Wikipedia wird unverzüglich tätig und entfernt den Inhalt, weiterhin wird der Nutzer von der Nutzung der Plattform ausgeschlossen. Die Veränderung des Artikels „Holocaust“ wird daraufhin von Wikipedia autorisierten Administratoren vorbehalten. In den Quelltext des Artikels wird zudem folgender Hinweis eingefügt: „<!--HINWEIS: Die Leugnung des Holocaust ist in der Bundesrepublik Deutschland nach § 130 Abs. 3 [[StGB]] – [[Volksverhetzung]] und § 189 StGB – Verunglimpfung des Andenkens Verstorbener STRAFBAR: ebenso in verschiedenen anderen Ländern. Die IP-Adressen der Benutzer, die diesen Artikel so verändern, dass sie gegen das Strafrecht verstoßen, den Holocaust leugnen oder die Leugnung unterstützen, werden AUFGEZEICHNET und SOFORT GESPERRT. Der Artikel steht unter DAUERNDER BEOBACHTUNG.--->“.

Begutachtung:

Wikipedia.de wird von einem in Deutschland ansässigen Hostprovider betrieben. Aus § 3 TMG folgt eine Unterwerfung des Falles unter deutsches Rechts. Die Äußerungen des X sind demnach nach § 130 StGB strafbar. Da Wikipedia hauptsächlich und in diesem Fall speziell, fremde Inhalte zum Abruf bereithält, ist sie als Hostprovider einzuordnen.

Wikipedia wurde zudem umgehend nach Erlangen von Kenntnis des Inhaltes (eine Kenntnis über die Rechtswidrigkeit geht hiermit einher, da er gegen allgemeine Gesetze verstößt) tätig und entfernte diesen. Hiermit wäre er abschließend durch § 10 Telemediengesetz (TMG) vor weiterer Verantwortlichkeit geschützt.

Jedoch geht Wikipedia ehrhaft weiter, sperrt den Artikel für Dritte und behält dessen Bearbeitung von Wikipedia autorisierten „Administratoren“ vor. Außerdem bekundet Wikipedia ausdrücklich, dass der Artikel von nun an unter „dauernder Beobachtung“ steht. Dies führt unglücklicherweise zu dem Paradoxon, dass Wikipedia Gefahr läuft durch dieses Handeln den Schutzmechanismus des § 10 TMG auszuhebeln. Zum einen könnten die Inhalte durch die ständige Überwachung als zu-eigen-gemacht angesehen werden, zum anderen ließe sich argumentieren, dass die Administratoren Wikipedia nach § 10 Satz 2 unterstehen. Würde ein Administrator nun den Tatbestand der Volksverhetzung erfüllen, ist Wikipedia möglicherweise vollkommen verantwortlich.

Wikipedia trägt in besonderem Maß zur Erfüllung des Interesses der Allgemeinheit an freiem Informationsaustausch über das Internet bei. Auch im Bezug auf Verletzungen von hochwertigen Rechtsgütern setzt es seine Möglichkeiten zur Verhinderung beispielhaft ein. Doch ist dies keinesfalls durch gesetzliche Anreize motiviert, sondern im Gegenteil, Wikipedia gefährdet sich durch diese Ausschöpfung der Möglichkeiten.

Videos mit urheberrechtlich geschütztem Inhalt auf myvideo.de

Sachverhalt:

Internetnutzer X hat sich auf der Videohostingseite myvideo.de angemeldet. Die Seite bietet Nutzern die Möglichkeit, Videos beliebigen Formats hochzuladen und öffentlich zugänglich zu machen. Nutzer X lädt ein Video von sich hoch in dem er Tanz- und Mundbewegungen zu einem Lied einer bekannten deutschen Band macht. Dieses Lied wird unverändert über die Tonspur des Videos wiedergegeben. Der Band fällt das Video auf und sie informiert myvideo.de über den „Melden“-Link auf der entsprechenden Seite. Dem Supportangestellten ist das Lied unbekannt, er reagiert nicht auf die Meldung. Darauf hin informiert die Band myvideo über ihr Urheberrecht und verlangt zudem Unterlassung der Wiederholung von myvideo als Störer. Das Video wird von der Seite entfernt. Einige Tage später lädt X das gleiche Video mit gleichem Titel erneut hoch. Myvideo pflegt keine technisch unterstützte Suche, lässt jedoch Stichproben von

einen Supportmitarbeiter durchführen, der sich täglich vier Stunden dieser Aufgabe widmet. Der Nutzer wurde zudem beim ersten Verstoß per Email informiert, dass erneute Hochladen des Videos zu unterlassen. Nach dem bekannt werden des zweiten Verstoßes wurde sein Profil gelöscht.

Begutachtung:

Auch wenn myvideo.de offiziell von einer rumänischen Firma betrieben wird, so ist das gesamte Portal doch seinem Wesen nach auf den deutschen Markt gerichtet. Die deutsche Band kann so unter Ausnutzung des Schutzlandprinzips Ansprüche aus dem Urheberrecht geltend machen. Myvideo ist weiterhin als Hostprovider einzustufen. Es ist fraglich, ob myvideo bereits bei der ersten Meldung hätte tätig werden müssen. Es kommt hier darauf an, ob nachgewiesen werden kann, dass der Supportmitarbeiter tatsächlich Unkenntnis von der Rechtswidrigkeit des Videos hatte. Da myvideo.de jedoch zumindest bei der zweiten Meldung unverzüglich tätig wurde, bleibt der Schutz des § 10 TMG erhalten. Dieser erstreckt sich jedoch nicht auf den Unterlassungsanspruch, es muss also eine Abwägung der Prüfungsmaßnahmen erfolgen um festzustellen, ob myvideo die Wiederholung der Tat zuzurechnen ist.

Das beeinträchtigte Rechtsgut ist nur von geringem Wert. Die Betrachtung des Videos kann nicht als Substitution für den Kauf des Liedes auf CD gesehen werden. Im Gegenteil ist das Video der Förderung der Bekanntheit der Band zuträglich. Dies muss die Anforderungen an myvideo schwächen. Auf der anderen Seite lässt sich auf der myvideo-Webseite kein eindeutiger Hinweis bezüglich Urheberrechtsverletzungen finden. Durch den expliziten Aufruf an die Nutzer auch „Werbespots“ hochzuladen (welche ja grundsätzlich urheberrechtlich geschützt sind) könnte angenommen werden, dass myvideo ein latentes Interesse daran hegt, dass von Nutzern auch geschützte Werk hochgeladen werden. Dies bestärkt die Anforderungen leicht, wird jedoch durch die Informationsemail an X wieder relativiert.

Das allgemeine Interesse an der Existenz der Dienstleistung von myvideo ist sicherlich nicht so hoch einzuordnen wie im Falle von Wikipedia, aber vorhanden – was die Zahl der Nutzer bestätigt. Die Anforderungen müssen also weiter abgeschwächt werden.

Die Band selbst hat Interesse, über Ihre Bekanntheit im Netz informiert zu sein, es kann ihr deswegen zugemutet werden selbst gelegentlich auf einschlägigen Videoseiten nach

dem Auftauchen ihres Namens zu suchen. Dies schwächt ebenfalls die Anforderungen an myvideo.

Es muss also zu dem Ergebnis gekommen werden, dass die gelegentlichen Stichproben durch einen halbtags allein hierfür tätigen Supportangestellten unter Effizienzkriterien ausreichend sind. Die Information an den Nutzer und die Löschung seines Profils stellen ausreichende Sanktionsmaßnahmen dar. Myvideo muss keine Verletzung von Prüfungspflichten gegen sich gelten lassen, haftet somit nicht für die Folgen des Unterlassungsanspruchs.

Abwandlung:

Es handelte sich bei dem Video um ein komplett geschütztes Musikvideo. Weiterhin sind in der Vergangenheit bereits mehrere solcher Videos der Band angemahnt und entfernt worden.

Begutachtung:

Die Wertigkeit des Rechtsgutes und die Gefahr der Verletzung sind nun entsprechend höher. Myvideo hätte die Suche des Supports Erfolg versprechender gestalten müssen. So hätte ein spezielles Suchsystem für den Support eingerichtet werden müssen über das dieser informiert wird, sobald ein Video, dessen Titel den Namen der Band enthält, hochgeladen wurde. Außerdem hätte dem Nutzer mit konkreten rechtlichen Konsequenzen gedroht werden müssen. Myvideo müsste in diesem Fall die Haftung für die Zwangsmaßnahmen der Unterlassung tragen.

Ehrenwörtliche Erklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit

„Prüfungspflichten und -möglichkeiten von Host Providern im Hinblick auf Content“

selbst angefertigt habe. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder nicht veröffentlichten Schriften entnommen wurden, sind als solche kenntlich gemacht. Die Arbeit hat in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegen und wurde zuvor noch nie veröffentlicht.

Hattenheim, den 07. Februar 2008

David Dell