Interessenverband des Video- und
Medienfachhandels in Deutschland

Verein zur Förderung der
Rechte im Internet e.V.

Stellungnahme zum

Referentenentwurf 2.TMGÄndG

8. April 2015

I. Kurzfassung

1.) Haftung der WLAN-Betreiber (§ 8 TMG)

Wir begrüßen das Ziel, die Möglichkeiten eines freien WLAN-Zugriffs zu stärken. Ebenso erscheint es sinnvoll, eine Haftungsfreistellung nur bei Erfüllung von Sorgfaltspflichten zu genehmigen. Dieses Ziel muss aber mit den zusätzlichen Gefahren für die illegale Verbreitung urheberrechtlich geschützter Inhalte abgewogen werden.
Diese Abwägung findet nicht statt. Die vorgesehenen Sorgfaltspflichten ermöglichen eine Gestaltung, die jegliche Verfolgung der Verletzung von Urheberrechten in Tauschbörsen (P2P) verhindern kann. Damit verstößt die Regelung auch gegen das Europäische Recht.

Wir schlagen vor, dass nur derjenige, der aktiv etwas gegen eine illegale Nutzung seines Anschlusses unternimmt, mit einer Haftungsfreistellung belohnt wird. Wir empfehlen deshalb die Aufnahme zwei weiterer Sorgfaltspflichten, von denen eine genutzt werden muss:

- Erfassung von Name, Anschrift sowie Zeit der Nutzung
- Filter und andere technische Maßnahmen

2.) Haftung der Hostprovider (§ 10 TMG)

Das Ziel die Haftungsprivilegierung von Angeboten einzuschränken, die fast ausnahmslos der Verbreitung illegaler Inhalte dienen, findet unsere volle Unterstützung in der Form, wie es im Koalitionsvertrag vereinbart wurde. Der mit diesem Entwurf vorgelegte Vorschlag erreicht das Ziel des Koalitionsvertrages nicht. Die vorgeschlagenen Kriterien sind kaum nutzbar.

Anstatt unsinniger Kriterien wäre es sinnvoll, wie bei den WLAN-Betreibern, Sorgfaltspflichten vorzusehen, bei deren Nichteinhaltung die Haftungsprivilegien verloren gehen. Dazu gibt es entsprechende Ansätze der Rechtssprechung. Zusätzlich können die Anonymität der Anbieter und der reale Umgang mit Löschungsanforderungen berücksichtigt werden. Eine entsprechende Systematik wird vorgeschlagen.

Eine Einschränkung der Haftungsprivilegierung von File-Hostern, die (fast ausnahmslos) anonym agieren, ist im Endeffekt ohne weitere Maßnahmen wenig hilfreich. Mögliche Ansprüche sind mangels ladungsfähiger Anschrift in der Regel gar nicht durchsetzbar.

Deshalb muss auch die nächste Stufe mit in die Verantwortung gezogen werden, die Datacenter, welche die Server für diese Dienste betreiben. Wenn nach den neuen rechtlichen Kriterien ein Angebot die Haftungsprivilegierung verliert, dann muss für die Datacenter gelten, dass dieses illegale Angebot nicht weiter verbreitet werden darf und ein entsprechender Löschungsanspruch besteht.

Die im Koalitionsvertrag im selben Satz vorgesehene Einschränkung der Werbeeinnahmen dieser Angebote wurde in diesem Entwurf nicht bearbeitet. Wir verweisen insoweit auf unsere Vorschläge zur aktuellen UWG-Novelle.

II. Haftung der WLAN-Betreiber (§ 8 TMG)

Wir begrüßen das Ziel, die Möglichkeiten eines freien WLAN-Zugriffs zu stärken. Ebenso erscheint es sinnvoll, eine Haftungsfreistellung nur bei Erfüllung von Sorgfaltspflichten zu genehmigen.

Dieses Ziel muss aber mit den zusätzlichen Gefahren für die illegale Verbreitung urheberrechtlich geschützter Inhalte abgewogen werden.

1.) Urheberrechtsverstöße und WLAN

Im privaten Bereich kann gar nicht zwischen Verstößen über WLAN oder LAN-Verbindung unterschieden werden. Man kann von außen nicht feststellen, wie die einzelnen Rechner im Haushalt angeschlossen sind.
Da die Tauschbörsenprogramme auch zeitversetzt arbeiten können, bietet nicht einmal eine häusliche Abwesenheit ein Anhaltspunkt. Der angebliche WLAN-Bezug kann also oft eine Ausrede darstellen.

Auch im gewerblichen Bereich besteht ein massives Problem der Bewertung der Sachlage. Bei vielen Gaststätten oder Kleinbetrieben ist oft gar nicht ersichtlich, ob es sich um einen gewerblichen Anschluss handelt.
Wenn es sich eindeutig um ein Unternehmen handelt, mahnen einige Anwälte nicht ab oder verfolgen die Fälle wegen der rechtlichen Unsicherheiten nicht weiter, wenn es Hinweise auf die Nutzung eines WLANs gibt. Insoweit sind auch Äußerungen von WLAN-Betreibern, dass es keine Probleme gäbe, mit Vorsicht zu genießen.
Vielmehr gibt es deutliche Hinweise darauf, dass öffentliche und anonyme WLAN-Zugänge überproportional häufig für Urheberrechtsverletzungen genutzt werden. Etwa 10 Prozent aller Rechtsverletzungen sollen über WLAN-Angebote erfolgen, die eine anonyme Nutzung ermöglichen.

2.) Zu den Regelungen des Referentenentwurfs

Wir halten eine rechtliche Regelung für angemessen, die sowohl eine weitere Verbreitung von offenen WLANs nicht behindert und andererseits nicht dazu führt, dass annähernd jegliche Rechtsverletzung mit der Ausrede WLAN unverfolgbar wird.

Dieses Ziel erreicht der vorliegende Vorschlag nicht. Die vorgesehenen Sorgfaltspflichten sind unzureichend:

a) Verschlüsselung:

Eine Verschlüsselung kann den unbefugten Zugang zum WLAN in der Regel verhindern. Wenn aber über einen längeren Zeitraum in einem gewerblichen Betrieb immer der gleiche Schlüssel verwendet wird, ist dieser bald so bekannt, dass man eher von einer offenen Tür als von einem verschlossen Zugang sprechen muss.

b) Erklärung:

Eine Erklärung, keine Rechtsverletzungen zu begehen, ist nicht sehr bindend, wenn es keine Sanktionen gibt.
Dies sieht auch das LG Hamburg[1] in dem Fall eines WLAN-Betreibers so:

> „Eine vertragliche Bindung und Belehrung allein erweist sich unter den Umständen des vorliegenden Falles als nicht ausreichend effektive Maßnahme gegen eigenverantwortliche Urheberrechtsverletzungen des Vertragspartners der V.-Beklagten. Grund dafür ist, dass die V-Beklagte – wie in der Widerspruchsverhandlung erörtert – ihren Kunden den Internetzugang bewusst unter Wahrung der Anonymität der Kunden überlässt. Wenn sich aber der Kunde bewusst ist, dass er seine personenbezogenen Daten nicht hat preisgeben müssen, so ist ihm auch bewusst, dass die Wahrscheinlichkeit einer nachträglichen Ermittlung seiner Identität äußerst gering ist. Unter dieser Voraussetzung braucht er vertragliche Sanktionen der V.-Beklagten kaum zu fürchten;“

c) Namen:

Ein Name alleine reicht nicht für die Verfolgung von Rechtsverletzungen. Gerichte wünschen eine ladungsfähige Anschrift.

Im Ergebnis kann der jeweilige Anschlussinhaber nach diesem Entwurf problemlos dafür sorgen, dass er nicht einmal als Täter zur Unterlassung verpflichtet ist. Insbesondere die gewerblichen WLANs können vom Kunden völlig ohne Restriktionen für den Bezug eigentlich urheberrechtlich geschützter Inhalte genutzt werden.
Mit der Erfüllung von Sorgfaltspflichten, die eine illegale Nutzung nicht verhindern, haben die Rechteinhaber keine Möglichkeit mehr Unterlassungsansprüche durchzusetzen. Da somit auch die Durchsetzung europarechtlich gebotener Maßnahmen:

> Artikel 8 (3) der Richtlinie 2001/29:
> „Die Mitgliedstaaten stellen sicher, dass die Rechtsinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden.“[2]

unmöglich wird, dürfte dieser Teil des Referentenentwurfs mit dem europäischen Recht nicht vereinbar sein.

Dies wird eine massive Stärkung der Nutzung von P2P-Netzwerken bedeuten und es ist abzusehen, dass die in Deutschland gesunkene Nutzung dieser illegalen Angebotsform wieder massiv steigen wird. Dass die Nutzer illegaler Inhalte in hohem Maße Wege bzw. Angebote nutzen, die nicht verfolgbar sind, zeigt die Abwanderung der Telekomkunden zu Vodafone.[3]

[1] LG Hamburg, Urteil vom 13.1.2015, Aktz.: 310 O 163/14

[2] Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft; Vgl. auch EuGH, 27.3.2014; C-314/12 UPC Telekabel

[3] www.webschauder.de/raubkopierer-lieben-hansenet-und-vodafone-telekom-verliert-weiterhin-marktanteile/

3.) Ergänzung der Sorgfaltspflichten

Nur derjenige, der aktiv etwas gegen eine illegale Nutzung seines Anschlusses unternimmt, sollte mit einer Haftungsfreistellung belohnt werden. Wir empfehlen deshalb die Aufnahme zwei weiterer Sorgfaltspflichten, von denen mindestens eine genutzt werden muss:

a) Erfassung von Name, Anschrift sowie Zeit der Nutzung

Mit der Erfassung von Nutzungszeitraum, Name und Anschrift der jeweiligen Nutzer gibt es zumindest die Möglichkeit, den jeweiligen Täter in einem Teil der Fälle verfolgen zu können. Für Anbieter, die diese Mühe scheuen, gibt es günstige Hotspotangebote, bei denen der Anbieter die Registrierung übernimmt.
Ergänzend muss sichergestellt werden, dass die Auskunftsansprüche des § 101 UrhR in WLAN-Fällen auch bei privaten Personen anwendbar sind.

b) Filter und andere technische Maßnahmen

Der Gefahr einer Nutzung illegaler Angebote kann auch mit Filtern reduziert werden. Bei vielen handelsüblichen Routern (z. Bsp. FritzBox), ist es möglich Gastzugänge zu konfigurieren und die Nutzung problematischer Protokolle auszuschließen. Urheberrechtsverletzungen über Tauschbörsen könnten somit verhindert werden. Auch das BPJM-Modul mit jugendschutzrechtlich bedenklichen Seiten ist in dem System enthalten, so würde manch eine strafrechtlich relevante Seite somit auch gesperrt.

Es wäre sinnvoll geprüfte Technologien einzuführen, bei denen automatisch eine Haftungsfreistellung erfolgt. Im Bereich des Jugendschutzes gibt es solche Anerkennungen durch die Kommission für Jugendmedienschutz (KJM)[4]. Dabei könnte es sich anbieten, die Nutzer solcher Technologien für maximal ein Jahr generell von der Haftung freizustellen und danach nur noch, wenn die verwendeten Technologie im Rahmen einer anerkannten Selbstkontrolle oder von einer anderen Institution anerkannt wurden.

4.) Verantwortlichkeit

Bei Nichterfüllung der Sorgfaltspflichten besteht ein direkter Unterlassungsanspruch. Dieser wird aber dadurch ausgehebelt, dass die Sorgfaltspflichten kaum die Nutzung der WLANs zu Urheberrechtsverletzungen verhindern. Deshalb bedarf es der zusätzlich vorgeschlagenen Sorgfaltspflichten.

Aus unserer Sicht sollten WLAN-Angebote ohne ausreichende Schutzmaßnahmen auch zu einem Schadensersatz verpflichtet werden können. Eine generelle Freistellung über den § 8 Abs. 3 sollte nicht erfolgen.

[4] Vgl. § 5 Abs. 3 JMStV und www.kjm-online.de/telemedien/jugendschutzprogramme.html

III. Haftung der Hostprovider (§ 10 TMG)

Das Ziel die Haftungsprivilegierung von Angeboten einzuschränken, die fast ausnahmslos der Verbreitung illegaler Inhalte dienen, findet unsere volle Unterstützung in der Form, wie es im Koalitionsvertrag vereinbart wurde:

> „Wir wollen die Rechtsdurchsetzung insbesondere gegenüber Plattformen verbessern, deren Geschäftsmodell im Wesentlichen auf der Verletzung von Urheberrechten aufbaut. Wir werden dafür sorgen, **dass sich solche Diensteanbieter nicht länger auf das Haftungsprivileg, das sie als sogenannte Hostprovider genießen, zurückziehen können** und insbesondere keine Werbeeinnahmen mehr erhalten."

1.) Zu den Regelungen des Referentenentwurfs

Der mit diesem Entwurf vorgelegte Vorschlag erreicht das Ziel des Koalitionsvertrages nicht. Die vorgeschlagenen Kriterien sind kaum nutzbar:

a) Überwiegende Zahl der gespeicherten Informationen

Dieser Beweis ist unmöglich. Man kann feststellen, dass Millionen von illegalen Daten bei einem solchen Hoster liegen. Um aber eine vermeintlich überwiegende Mehrheit der gespeicherten Informationen zu belegen, benötigt man einen Zugriff auf die Rechner, dieser liegt aber nicht vor.
Im Zweifel würde der Anbieter einfach einige Milliarden Dateien mit Inhalten abspeichern, die niemanden interessieren und auch nie genutzt werden. Er könnte damit aber belegen, dass die von Dritten erkannten illegalen Dateien weniger als 50% betragen.
Über aufwendige Untersuchungen hat man bei drei großen File-Hostern herausgefunden, dass diese von den Kunden fast nur für den Bezug illegaler Inhalte genutzt werden[5]. Dies ist aber nur begrenzt möglich, da die Nutzer des der Untersuchung zu Grunde liegenden Tools inzwischen gewarnt sind, dass man feststellen kann, dass sie sich illegal verhalten. Es ist somit fraglich, ob eine solche Untersuchung wiederholbar wäre. Zudem wären die Kosten einer solchen Untersuchung unzumutbar.

b) Förderung der Gefahr durch eigene Maßnahmen

Dieses Kriterium bleibt unklar. Wesentlicher Ansatzpunkt der Förderung rechtswidriger Nutzung sind Prämien, die den Uploadern zur Verfügung gestellt werden und deren Höhe von der Anzahl der Downloads abhängen. Gerichtlich wird dies unterschiedlich gesehen. Ob dies hier gemeint ist bleibt offen.

[5] GfK / OpSec: Studie zur Nutzung von Sharehostern, 2013, www.webschauder.de/erste-studie-zur-nutzung-von-sharehostern/ oder www.faz.net/aktuell/feuilleton/medien/sharehoster-studie-komm-auf-meine-festplatte-12113447.html

c) Werbung mit Nichtverfolgbarkeit

Uns sind solche Werbeaussagen von Hostern im letzten Jahr nicht aufgefallen. Spätestens mit Inkrafttreten des Gesetzes würden solche Werbeaussagen entfernt und nur noch über Dritte auf anderen Seiten platziert.

d) Keine Möglichkeit der Löschung

Dieses Kriterium wird in Satz zwei der Begründung in zwei Bedingungen aufgegliedert:

- Die Möglichkeit den Betroffenen davon in Kenntnis zu setzen.
  Diese Bedingung wäre erfüllt sobald eine E-Mail-Adresse angegeben würde.
- Der Dienstanbieter muss die Möglichkeit haben zu löschen.
  Davon ist grundsätzlich auszugehen. Der Verantwortliche hat eigentlich immer Zugriff auf seinen Rechner. Selbst wenn dies einmal nicht der Fall sein sollte, wäre dies für einen Außenstehenden nicht nachweisbar.

De facto ist es bei diesem Kriterium egal, ob der Hoster löscht. Es reicht aus, wenn er eine Löschung anbietet.

Im Ergebnis sind die hier genutzten Kriterien so formuliert, dass sie nicht anwendbar sind. Das Ziel des Koalitionsvertrags wird nicht annähernd erreicht.

2.) Nutzung möglicher Sorgfaltspflichten

Anstatt unsinniger Kriterien wäre es sinnvoll, wie im Teil zur WLAN-Haftung, Sorgfaltspflichten vorzusehen, bei deren Nichteinhaltung die Haftungsprivilegien verloren gehen:

a) Ansätze der Rechtssprechung

Der Bundesgerichtshof hat mit der Entscheidung File-Hosting-Dienst festgelegt, dass einem File-Hoster, der durch sein konkretes Geschäftsmodell Urheberrechtsverletzungen in erheblichem Umfang Vorschub leistet, eine umfassende regelmäßige Kontrolle der Linksammlungen, die auf seinen Dienst verweisen, zuzumuten ist. Sharehoster, die diese Bedingungen nicht erfüllen, sind als illegal zu betrachten.
In einer Studie aus dem Jahr 2014 wurde festgestellt, dass nur das damals verklagte Unternehmen Rapidshare auch diese Linkkontrollen durchführte.[6]

Das LG München ging kürzlich noch einen Schritt weiter, dort reichte die häufigere Benennung eines illegalen Portals aus, um die Haftung auch für nicht genannte Medieninhalte zu ermöglichen.[7]

[6] FDS / OpSec, Studie zur Nutzung von Zahlungsdienstleistern bei der illegalen Verbreitung urheberrechtlich geschützter Werke (Zahlungsstudie), 2014, Seite 16; www.webschauder.de/downloads/zahlungsstudie.pdf
[7] LG München 1, Urteil vom 11.07.2014, Az. 21 O 854/13; www.raschlegal.de/news/lg-muenchen-i-praezisiert-voraussetzungen-einer-schadensersatzhaftung-des-hostproviders/

Entsprechend der BGH-Entscheidung „Jugendgefährdende Medien bei eBay“[8] kann man auch erwarten, dass die jeweiligen Hoster dafür Sorge tragen müssen, dass der Uploader eines gemeldeten Verstoßes keine weiteren urhebrechtlichen Verstöße mehr begehen kann.

b) Löschdauer

Hoster sind verpflichtet, gemeldete illegale Inhalte zu löschen. Wer dies nicht tut, haftet. In welchem Zeitraum sie löschen müssen bleibt offen. Manche Hoster ermöglichen eine sofortige Löschung über Schnittstellen, andere schaffen die Löschungen in weniger als 6 Stunden. Eine Löschdauer über 8 Stunden könnte man als eines der Kriterien nehmen. Wer langsamer löscht haftet.
Man könnte dies mit einer Anforderung an die Form der Notice-and-Take-Down-Benachrichtigungen (NTD) verbinden.

c) Anonymität / Verschleierung

Oft werden die Dienste anonym angeboten.[9] Die Hoster selber agieren mit Scheinadressen und versuchen Ihre Identität zu verschleiern. Um Auskunftsrechte zu unterlaufen, erfassen Hoster die Identität der Uploader gar nicht.
Dies könnte man als Kriterium nutzen: Wenn der Hoster zum Uploader oder das Rechenzentrum zu seinem Kunden dem Hoster bei berechtigten Auskunftsanfragen keine zur Verfolgung nutzbaren Angaben macht, muss er selber für das Angebot haften.

d) Vorliegender BDWi-Vorschlag

Im Rahmen der UWG-Novelle hat der BDWi vorgeschlagen, Werbung und Finanztransfers zu illegalen Angeboten als Tatbestände unlauteren Wettbewerbs in das UWG aufzunehmen und folgende Kriterien anzulegen:
„Da aber das Verhältnis von legalen zu illegalen Angeboten für Außenstehende nur bedingt feststellbar ist, bedarf es einiger Ansatzpunkte zur Einstufung als illegales Angebot.
Diese können u.a. sein:

- Legale Inhalte sind bei dem Internetangebot nicht in größerem Umfang zu erkennen.
- Das Internetangebot agiert anonym bzw. identifiziert nicht die Betreiber des Angebotes (keine ladungsfähige Adresse im Impressum, keine Nennung von vertretungsberechtigten Personen usw.).
- Binnen eines Jahres sind mindestens 500 illegale Inhalte (Speicherungen, Verlinkungen etc.) dieser Seite belegbar.
- Dauerhaftes illegales Glücksspiel- oder Pornographieangebot, welches auch von Kindern und Jugendlichen genutzt werden kann.“

[8] BGH: Urteil vom 12. Juli 2007 – I ZR 18/04 – Jugendgefährdende Medien bei eBay
[9] Zahlungsstudie, S. 15

3. Vorschlag einer Systematik von Sorgfaltspflichten

Die Haftungsprivilegierung verliert, wer

- gegen die vom BGH erlassen Prüfpflichten verstößt (insbesondere Kontrollen von Linksammlungen und Kontrolle von aufgefallenen Uploaders)

oder

- auf (formalisierte) NTD-Hinweise nicht binnen 48 Stunden löscht

oder

- dauerhaft ein illegales Glücksspiel- oder Pornographieangebot deutschen Nutzern anbietet ohne dafür Sorge zu tragen, dass Kinder und Jugendliche diese nicht nutzen können (Verweis auf geschlossen Benutzergruppe)

oder

- ein Angebot betreibt, bei dem binnen eines Jahres mindestens 500 illegale Inhalte (Speicherungen, Verlinkungen etc.) auf dem Angebot belegbar sind und bei dem außerdem legale Inhalte nicht in größerem Umfang offensichtlich zu erkennen sind sofern eine der zusätzlichen Bedingungen erfüllt ist:
    - Das Internetangebot agiert anonym bzw. identifiziert nicht die Betreiber des Angebotes (Keine ausreichende Erfüllung der allgemeinen Informationspflichten nach § 5 TMG).
    - Es erfasst Name und Anschrift der Uploader nicht.
    - Es ist mehrfach nicht in der Lage ein Auskunftsbegehren nach § 101 UrhR mit einer ladungsfähigen Anschrift zu erfüllen.
    - Es löscht (formalisierte) NTD-Ansprüche nicht binnen 8 Stunden.

Es muss klargestellt werden, dass es in einem Verfahren eines Rechteinhabers gegen einen solchen Hoster, der beklagte Hoster dem Vorwurf nicht dadurch begegnen kann, dass dieser Rechteinhaber gleichartige Verstöße bei anderen Rechteinhabern nicht belegen kann. Ansonsten diskutieren die Gerichte, ob denn wirklich der Rest der Inhalte illegal ist. Den Nachweis der fehlenden Rechte anderer Firmen kann aber ein einzelner Rechteinhaber gar nicht erfüllen.

4.) Grenzen des Ansatzes / Notwendige Erwähnung der Datacenter

Eine Einschränkung der Haftungsprivilegierung von File-Hostern, die (fast ausnahmslos) anonym agieren, ist im Endeffekt ohne weitere Maßnahmen wenig hilfreich. Mögliche Ansprüche sind mangels ladungsfähiger Anschrift in der Regel gar nicht durchsetzbar.

Diese Geschäftsmodelle, die im Wesentlichen auf der Verletzung von Rechten basieren, bieten den Uploadern Speicherplatz an. Dazu nutzen sie aber keine eigenen Serversysteme sondern kaufen diese Serverleistung bei Hostinganbieter ein, die diese Server betreiben und mit dem Internet verbinden.[10] Aus Gründen der besseren Abgrenzbarkeit werden diese Hoster im Weiteren als Datacenter bezeichnet.

[10] Dies entspricht in etwa der Erstellung der Homepage eines Abgeordneten, der entsprechenden Speicherplatz bei einem Hoster anmietet.

Da die illegalen Angebote oft anonym agieren, muss auch die nächste Stufe mit in die Verantwortung gezogen werden, die Datacenter. Diese liegen meist in Europa und es handelt sich dabei keinesfalls um anonyme Unternehmen. Teilweise werden einzelne Server über Netzwerke betreut, sogenannte Content Delivery Networks (CDN). Diese organisieren den Datenverkehr mehrerer Server um die Auslastung zu optimieren und die Herkunft zu verschleiern)
Dabei ist auffallend, dass sich viele der illegalen Angebote bei einigen wenigen Datacentern befinden. Seriöse Datacenter, wie beispielsweise Strato, sind bisher nicht aufgefallen.[11]

Insoweit ist es notwendig, dass der Gesetzentwurf nicht nur auf die illegalen Share- und Videohoster abstellt, sondern klarstellt, dass ein Verlust der Haftungsprivilegierung ein Beweis für die Illegalität eines Angebotes ist. In der Folge haben die Betroffenen einen NTD-Anspruch gegenüber dem jeweiligen Datacenter oder CDNs (i.d.R. durch eine ASN identifizierbar) und zwar unabhängig davon

a) ob der bei ihnen angeschlossene Server vermietet ist oder angeblich dem Kunden gehört,
oder
b) ob eine direkte Verbindung zum Server besteht oder die Last auf verschiedene Server verteilt wird (Content Delivery Network).

Kurz gefasst: Wenn nach den neuen rechtlichen Kriterien ein Angebot die Haftungsprivilegierung verliert, dann muss für die Datacenter und CDNs gelten, dass dieses illegale Angebot nicht weiter verbreitet werden darf und ein entsprechender NTD-Anspruch besteht.

Der Fall, dass ein „normaler“ Speicherplatzanbieter ein Problem mit solchen Angeboten bekommt ist fast auszuschließen. Diese nutzen in der Regel Datacenter, die solche Angebote unterstützen. Aber selbst wenn ein Datacenter dafür genutzt würde, könnte es den NTD-Anspruch erfüllen und dem Dienst kündigen und könnte somit weder auf Unterlassung noch auf Schadensersatz in Anspruch genommen werden.

Im Falle von illegalen Angeboten aus den Bereichen Jugendschutz und Glücksspiel besteht natürlich auch die Möglichkeit, dass das Datacenter die Nutzung durch Deutsche über eine Geolokalisierung ausschließt (Vgl. LG Hamburg, Beschluss v. 20.06.2014, Az. 312 O 322/12[12]).

[11] www.webschauder.de/spielfilme-2014-wieder-dominiert-illegal-50-des-angebots-ueber-eco-mitglieder/
Zudem wurde festgestellt, dass eine nicht unerhebliche Anzahl der Datacenter für illegale Angebote Mitglied des Verbandes eco sind. Von den illegalen Angeboten der Top 25 File- und Videohostern befinden sich etwa 50 % der Dateien auf Datacentern (und CDNs) die Mitglied von eco sind.
[12] www.telemedicus.info/urteile/Internetrecht/1495-LG-Hamburg-Az-312-O-32212-Verstoss-gegen-Unterlassungsverfuegung-durch-Umgehung-einer-IP-Sperre.html

5.) Werbung

Die im Koalitionsvertrag ebenso vorgesehene Einschränkung der Werbeeinnahmen dieser Angebote wurde in diesem Entwurf nicht bearbeitet. Wir verweisen insoweit auf unsere Vorschläge zur aktuellen UWG-Novelle in der Anlage.

Der Bundesverband der Dienstleistungswirtschaft (BDWi) vertritt 20 Branchenverbände des tertiären Sektors, denen rund 100.000 Unternehmen mit mehr als 1,5 Millionen Mitarbeitern angehören. Das Thema des Geistigen Eigentums wird im Verband von dem Arbeitskreis Rechtewahrung im Internet behandelt.

Bundesverband der Dienstleistungswirtschaft (BDWi), Ralf-Michael Löttgen, Matthias Bannas, Universitätsstraße 2 – 3a, 10117 Berlin, Tel.: ..49-30-2888070, E-Mail: Bannas@bdwi-online.de; www.bdwi-online.de

Der Interessenverband des Video- und Medienfachhandels in Deutschland e.V. (IVD) vertritt als klassischer Berufsverband die Interessen von über 1.500 Video- und Medienfachgeschäften.

Interessenverband des Video- und Medienfachhandels in Deutschland e.V. (IVD), Jörg Weinrich, Hartwichstraße 15, 40547 Düsseldorf, Tel.: ..49-211-5773900, E-Mail: weinrich@ivd-online.de; www.ivd-online.de

Web-Guard - Verein zur Förderung der Rechte im Internet e.V. vertritt die Interessen von Filmprogrammanbietern und Gruppierungen des Videomarktes. Aufgabe des Vereins ist es Verstöße gegen das Urheberrecht, das Wettbewerbsrecht und den Jugendschutz im Internet zu verfolgen sowie innovative Ansätze zur Verfolgung der Rechtsverletzer zu entwickeln und zu testen, so zum Beispiel Auskunftsverfahren gegenüber Share-Hostern.

Web-Guard - Verein zur Förderung des Rechtsschutzes im Internet e.V., Jörg Weinrich, Hartwichstraße 15, 40547 Düsseldorf, Tel.: ..49-211-5773900, E-Mail: info@webguard-online.de; www.webguard-online.de