verbraucherzentrale
Bundesverband

7. April 2015

HAFTUNGSBEFREIUNG FÜR WLAN STÄRKEN

Referentenentwurf des Bundesministeriums für Wirtschaft und Energie für ein Zweites Gesetz zur Änderung des Telemediengesetzes – 2. TMGÄndG

Impressum

Verbraucherzentrale
Bundesverband e.V.

Markgrafenstraße 66

10969 Berlin

verbraucherzentrale
Bundesverband

Inhalt

I. Grundsätzliches

Der Verbraucherzentrale Bundesverband (vzbv) hält den vorliegenden Gesetzentwurf grundsätzlich für verfehlt, im Kern greifen die Regelungen zu kurz und orientieren sich nicht an den Anforderungen des digitalen Zeitalters.

Betreffs der vorgeschlagenen neuen Verpflichtungen für Access-Provider ist nicht nachvollziehbar, warum Verbraucher, die anderen über ein WLAN den anonymen Zugang zum Internet ermöglichen, für von Dritten begangene Urheberrechtsverletzungen im Rahmen der Störerhaftung verantwortlich sein sollen, während kommerzielle Anbieter von WLAN-Hotspots unter bestimmten Bedingungen haftungsbefreit sein sollen, auch wenn sie eine anonyme Nutzung zulassen. Plausibel wäre es im Lichte der von dem Gesetzesentwurf genannten Zielsetzung gewesen, umgekehrt an jene Akteure, die aus etwaigen Rechtsverletzungen einen kommerziellen Vorteil ziehen, höhere Anforderungen zu stellen als an jene, die dies nicht tun. Dass Verbraucher hingegen in Bezug auf Haftungsfragen rechtlich schlechter gestellt werden sollen als kommerzielle Anbieter, ist aus Sicht des vzbv inakzeptabel.

Ebenso verfehlt erscheint die Verschärfung der Voraussetzungen für eine Haftung der Hostprovider im zweiten Teil des Gesetzentwurfs. Dass in Zukunft statt des Nachweises tatsächlicher Kenntnis von Rechtsverletzungen eine gesetzliche Vermutung solcher Kenntnis ausreichen soll, um Hostprovider haftbar zu machen, erscheint als eilfertige Reaktion zum Schutz der Rechte an geistigem Eigentum, ohne dabei die Auswirkungen auf die gesellschaftliche und wirtschaftliche Bedeutung des Internets abzuwägen. Der Schaden dieser Regelung wird insbesondere darin bestehen, dass Hostprovider vermeintlich freiwillig diverse Inhalte löschen, deren rechtliche Bewertung sich ihrer Kenntnis entzieht, um von vornherein keine Angriffsfläche für Haftungsklagen zu bieten. Hier drohen eine freiwillige Selbstzensur und damit eine Privatisierung der Rechtsdurchsetzung.

Der vzbv bezweifelt, dass Verschärfungen der Haftungsregelungen für Access- und Hostprovider ein geeignetes Mittel sind, um gegen Urheberrechtsverstöße im Internet wirksam vorzugehen. Die Haftungsregelungen für Access- und Hostprovider zu verschärfen führt vielmehr zu einer eingeschränkten Verfügbarkeit von Internetzugängen sowie einer Erschwerung der Tätigkeit von Hostprovidern. Die vorgeschlagenen Regelungen sind zudem unvereinbar mit der Richtlinie über den Elektronischen Geschäftsverkehr (RL 2000/31/EG, E-Commerce-Richtlinie), stehen im Widerspruch zu Regelungen des TMG und des TKG und laufen den Entwürfen der Europäischen Kommission für eine Verordnung über

Maßnahmen zum europäischen Binnenmarkt der elektronischen Kommunikation und zur Verwirklichung des vernetzten Kontinents zuwider (2013/0309 (COD), Telecom Single Market Act).

II. zu § 8 TMG

Zu Absatz 3:

Der vzbv begrüßt die Klarstellung in Absatz 3, der zufolge WLAN-Anbieter als Diensteanbieter auch dem TMG unterfallen. Dies steht im Einklang mit der Rechtsprechung und scheint auch sachgerecht.

Zu Absatz 4:

Der vzbv hält es nicht für sachgerecht, Diensteanbietern Verpflichtungen oder Maßnahmen aufzuerlegen, um Rechtsverletzungen durch Nutzer zu verhindern. Anders als in der Begründung dargelegt, entspricht dies auch nicht der geltenden Rechtsprechung. So bezieht sich insbesondere das BGH-Urteil „Sommer Deines Lebens“ (BGH, Urteil vom 12.05.2010, Az. I ZR 121/08) gerade nicht auf bewusst an die Öffentlichkeit gerichtete WLANs und hierfür zumutbare Maßnahmen, sondern lediglich auf die Absicherung eines privaten Anschlusses gegen den unberechtigten Zugriff Dritter. Der BGH geht auch in seiner Urteilsbegründung mit keinem Wort auf die Haftungsfreistellung der Zugangsdiensteanbieter ein, sondern stellt lediglich fest, dass eine Haftungsfreistellung für Hostprovider nach § 10 TMG im strittigen Fall nicht in Frage komme. Einen privaten Anschlussinhaber trifft unstrittig eine sekundäre Darlegungslast, wenn er selbst als Täter nicht in Frage zu kommen behauptet – der BGH hat die entsprechenden Anforderungen in seinem BearShare-Urteil konkretisiert (Urteil vom 08.01.2014, Az. I ZR 169/12). Wenn hingegen Diensteanbieter einer unbestimmten und gegebenenfalls unbegrenzten Zahl von Dritten wissentlich und willentlich einen Zugang zum Internet eröffnen, handelt es sich um eine andere Konstellation. Tatsächlich hatte der BGH bislang keinen Fall zu entscheiden, bei dem etwa der Inhaber eines Cafés, das öffentliches WLAN anbietet, als Störer in Anspruch genommen worden wäre. Der Gesetzentwurf stellt in dieser Hinsicht also durchaus eine Verschärfung gegenüber der geltenden Rechtsprechung dar.

Aus Sicht des vzbv sind die vorgesehenen Maßnahmen (Pflicht zur Verschlüsselung sowie zur Einholung einer Absichtserklärung des Nutzers) unzumutbar, da die Grenze der Zumutbarkeit überschritten ist, wenn

das Geschäftsmodell erheblich beeinträchtigt wird. Die Auferlegung dieser Verpflichtungen schafft beträchtliche zusätzliche Hürden für die Nutzer und Anbieter des WLAN. Dadurch erschwert sich die geschäftliche Betätigung als Diensteanbieter erheblich und macht die Verpflichtungen unzumutbar.[1] Der Kreis potenzieller Anbieter und Nutzer der Hotspots wird sich durch die Erschwerung bei der Nutzung des Angebots verkleinern. Diese Wirkung auszugleichen, wird beträchtliche Investitionen der Anbieter erforderlich machen. Es wäre redlich, wenn der Gesetzentwurf die daraus entstehenden Kosten im Rahmen der Angaben zum Erfüllungsaufwand wenigstens erwähnen würde.

Der erwähnte Eingriff in die Rechte der Diensteanbieter kann im vorliegenden Fall kaum durch eine Verkehrssicherungspflicht begründet werden, da mit der Zugänglichmachung des Internets allein keine Gefahrenquelle eröffnet wird. Mit dem Dienstangebot geht keine erhöhte, über das allgemeine Lebensrisiko hinausgehende Gefahr eines Schadeneintritts ein, die allein Grundlage einer Verkehrssicherungspflicht sein könnte. Auch geht keine unmittelbare Gefahr von der technischen Einrichtung der Zugänglichmachung aus. Die Gefahr einer möglicherweise durch Dritte intentional begangenen Rechtsverletzung reicht hier nicht aus.[2]

Anders als im Fall einer unzureichenden Absicherung eines privaten Internetzugangs ist auch fraglich, ob einer Anwendung der Störerhaftung auf Diensteanbieter überhaupt vorgebeugt zu werden braucht oder ob sich eine solche Anwendung nicht ohnehin verbietet. Thomas Stadler hat dies ausführlich dargelegt:

„An diesem Punkt sollte man sich in Erinnerung rufen, dass die Versorgung mit einem Internetzugang letztlich eine Maßnahme der Daseinsvorsorge darstellt, ebenso wie die Versorgung mit Telefon oder dem Postdienst schon seit Jahrzehnten. Dass der Staat diese Leistung der Daseinsvorsorge heutzutage nicht mehr selbst erbringt, sondern dies von privaten Internet-Service-Providern erledigt wird, ist eine Folge der Privatisierung des Telekommunikationssektors. Würde nun der Staat selbst – in Erfüllung seiner Aufgabe der Daseinsvorsorge – einen flächendeckenden Internetzugang zur Verfügung stellen, so wäre dieser Zugang zwangsläufig für jedermann offen und frei und deshalb natürlich

[1] So auch, neben vielen anderen, Mantz/Sassenberg: Rechtsfragen beim Betrieb von öffentlichen WLAN-Hotspots, NJW 2014, Heft 49, S. 3537-3600.

[2] Vgl. hierzu Breyer, Verkehrssicherungspflichten von Internetdiensten im Lichte der Grundrechte, MMR 2009, Heft 1, Seite V-72.

auch mit der Gefahr von Urheberrechtsverletzungen durch Nutzer verbunden. Man würde bei einer solchen Ausgestaltung allerdings wohl kaum die Frage stellen, ob der Staat als Störer einer Urheberrechtsverletzung anzusehen ist."[3]

Von rechtlichen Argumenten abgesehen, wäre die vorgeschlagene Regelung auch technisch kontraproduktiv. Verschlüsselung ist ein sinnvolles Instrument, um die eigene Kommunikation zu schützen, jedoch nicht, um einen Dienst einer Öffentlichkeit zugänglich zu machen. Dies erschließt sich unmittelbar, wenn man sich vergegenwärtigt, dass zum Beispiel öffentliche Gebäude, etwa Ämter, in der Regel nicht abgeschlossen sind, weil sie dann der Öffentlichkeit nicht oder nur mit erheblichem Aufwand zugänglich wären. Genauso verhält es sich mit WLAN-Zugängen. Tatsächlich sind auch die öffentlichen Hotspots der kommerziellen Anbieter heutzutage nicht verschlüsselt, sondern setzen lediglich eine Anmeldung voraus, die jedoch erst für den Zugang zum Internet benötigt wird – mit dem Router selbst kann sich jeder Client, also jedes Endgerät, ohne weiteres verbinden. Wäre dem anders, hätten die Anbieter kaum eine Möglichkeit, den Nutzern einen Zugang zu eröffnen, da sie ihnen den Schlüssel für das WLAN nur außerhalb der elektronischen Kommunikation über dieses Netz zugänglich machen könnten, also beispielsweise per Brief. Dessen unbeschadet, ist aus Sicht des vzbv ein Ausbau der verschlüsselten Kommunikation über das Internet dringend erforderlich und sollte (als verpflichtende Option) bspw. für E-Mail-Anbieter gesetzlich vorgeschrieben werden.

Die zweite vorgesehen Maßnahme mit haftungsbefreiender Wirkung läuft aus Sicht des vzbv komplett leer. Der Nutzer soll erklären, dass er im Rahmen der Nutzung keine Rechtsverletzungen begehen wird. Sofern der Zugang anonym genutzt wird, was zumindest bei kommerziellen Betreibern weiterhin möglich sein soll, ist eine solche Erklärung folgenlos. Sofern der Nutzer sich zusätzlich namentlich registriert, wäre sie nur sinnvoll, wenn dann bei der Nutzung tatsächlich eine Speicherung der Bestands- und Kommunikationsdaten erfolgen würde. Dies würde nach derzeitiger Rechtslage gegen § 88 TKG (Fernmeldegeheimnis) sowie § 13 (6) TMG (Möglichkeit der anonymen Nutzung) verstoßen. Es wäre zudem mit der Rechtsprechung des Europäischen Gerichtshofs

[3] Stadler, AnwZert ITR 9/2010, Anm. 3. Auch Reto Mantz zieht eine Parallele zur Daseinsvorsorge. Er meint, dass auch ein Postdienstleister die Gefahr eröffne, dass er Briefe mit rechtsverletzendem Inhalt befördere und dadurch kausal an Rechtsverletzungen mitwirke. Mantz, Die Haftung des Betreibers eines WLan-Zugangs für die Handlungen seiner Nutzer, JurPC Web-Dok. 95/2010, Abs. 1-45.

zur Vorratsdatenspeicherung unvereinbar. Das Anliegen, Urheberrechtsverletzungen vorzubeugen, stellt zweifellos eines der schwächsten Argumente für eine Wiedereinführung der Vorratsdatenspeicherung dar, die der vzbv ohnehin für unvereinbar mit dieser Rechtsprechung hielte.

Sofern eine derartige Speicherung nicht beabsichtigt ist, die Vorgabe also wirkungslos bleiben soll, ist zu beachten, dass den Access-Providern auferlegte Maßnahmen zur Zugangserschwerung nach Ansicht des EuGH „hinreichend wirksam“ sein müssen, „um einen wirkungsvollen Schutz des betreffenden Grundrechts“, hier also des Rechts des geistigen Eigentums, „sicherzustellen „d.h., sie müssen bewirken, dass unerlaubte Zugriffe auf die Schutzgegenstände verhindert oder zumindest erschwert werden und dass die Internetnutzer, die die Dienste […] in Anspruch nehmen, zuverlässig davon abgehalten werden, auf die ihnen unter Verletzung des genannten Grundrechts zugänglich gemachten Schutzgegenstände zuzugreifen.“[4] Dies ist durch eine One-Click-Rechtstreue-Erklärung des Nutzers nicht gegeben.

Zuletzt sei darauf hingewiesen, dass die vorgeschlagene Regelung nicht vereinbar ist mit Art. 12 der E-Commerce-Richtlinie (Reine Durchleitung), der eine ausdrückliche Haftungsbefreiung der Access-Provider zwingend vorschreibt, sofern bestimmte Voraussetzungen erfüllt sind (Übermittlung nicht veranlasst, Adressat nicht ausgewählt, übermittelte Informationen nicht ausgewählt oder verändert). Auch die Vereinbarkeit mit Art. 15, demzufolge keine allgemeinen Maßnahmen auferlegt werden dürfen, erscheint zumindest fragwürdig.

Zu Absatz 5:

Verbraucher, die als Diensteanbieter Dritten ihren Internetzugang zur Verfügung stellen, sollen diesem Absatz zufolge zusätzlich zu den anderen Sicherungsmaßnahmen gewährleisten, dass sie den Namen derjenigen kennen, die ihr Angebot nutzen. Dieser Anforderung begegnen wiederum die oben bereits erwähnten datenschutzrechtlichen Bedenken (§ 88 TKG, § 13 (6) TMG, BVerfG, Az. 1 BvR 256/08 - unzulässige Vorratsdatenspeicherung). Die vorgeschlagene Regelung schießt zudem weit über ihr Ziel hinaus, da damit freie WLANs offenkundig unmöglich wären. Ein Verbraucher, der sein WLAN Dritten zur Nutzung überlassen will, ist schlicht nicht in der Lage, die Namen der Mitnutzer in Erfahrung zu bringen. Im Ergebnis handelt es sich also um eine Verunmöglichung

[4] EuGH, Urteil vom 27.03.2014, Az. C-314/12

wenn nicht des Angebots selbst, so doch der Erlangung einer Haftungsfreistellung. Abgesehen von der auch hier erwähnenswerten Unvereinbarkeit mit Art. 12 und 15 der E-Commerce-Richtlinie werden dadurch kommerzielle Anbieter, die derart strengen Anforderungen nicht unterliegen, gegenüber nichtkommerziellen bevorzugt. Das ist eine klare Diskriminierung der nicht-kommerziellen Diensteanbieter, ohne dass hierfür eine Rechtfertigung ersichtlich ist und deren Auswirkungen auf die Kommunikationsfreiheit auch grundrechtliche Bedenken begegnen.

III. zu § 10 TMG

Nach derzeitigem Recht sind Hostprovider von der Haftung für Rechtsverletzungen Dritter befreit, sofern sie von diesen keine Kenntnis haben. Der vorliegende Gesetzentwurf möchte nun eine gesetzliche Vermutungsregelung einführen. Das Kriterium der Kenntnis soll demnach erfüllt sein, „wenn es sich bei dem angebotenen Dienst um einen besonders gefahrgeneigten Dienst handelt“. Im Ergebnis wird dadurch die haftungsrelevante Voraussetzung der Kenntnis von einem konkreten Rechtsverstoß durch eine unter bestimmten Bedingungen vorliegende gesetzliche Vermutung über eine solche Kenntnis ersetzt. Dies verstößt nach Auffassung des vzbv gegen Art. 14 (Hosting) der E-Commerce-Richtlinie.

Nach Dafürhalten des Entwurfs soll ein Hostprovider sich zukünftig selbst beurteilen, nämlich im Hinblick darauf, ob sein Angebot besonders gefahrgeneigt ist oder nicht. Dabei ist insbesondere das erste Kriterium zur Feststellung besonderer Gefahrenneigung bedenklich: wenn „die Speicherung oder Verwendung der weit überwiegenden Zahl der gespeicherten Informationen rechtswidrig erfolgt“. Der Hostprovider ist gerade darum haftungsprivilegiert, weil er ohne Hinweis auf konkrete Rechtsverletzungen die Rechtmäßigkeit von Angeboten Dritter auf seiner Plattform regelmäßig nicht beurteilen kann. Wenn ihm in Zukunft dennoch Kenntnis von den Rechtsverletzungen unterstellt werden kann, wäre er gezwungen, die Angebote regelmäßig zu überwachen (was ein Verstoß gegen Art. 15 der E-Commerce-Richtlinie wäre) und aufgrund nicht näher benannter Kriterien zu entscheiden, ob diese vermutlich in „der weit überwiegenden Zahl“ rechtswidrig sind oder nicht. Nur so könnte er einer Qualifikation als „besonders gefahrgeneigter Dienst“ und damit dem Verlust seiner Haftungsprivilegierung entgehen.

Eine solche Verschärfung der Hostprovider-Haftung geht weit über das BGH-Urteil zu Rapidshare (Urteil vom 15.08.2013, Az. I ZR 80/12) hinaus. Hier hat das Gericht eine besondere Gefahrengeneigtheit eines

Dienstes erst angenommen, wenn das konkrete Geschäftsmodell von vornherein auf Rechtsverletzungen durch die Nutzer angelegt ist oder der Gewerbetreibende durch eigene Maßnahmen die Gefahr einer rechtsverletzenden Nutzung fördert. Eine schlicht anhand der Zahl der vermutlich widerrechtlich gespeicherten Informationen vermutete Gefahrgeneigtheit lässt diese Kriterien außer Acht und führt zu einer Überforderung und übereilten Zensur durch die Hostprovider.

Der EuGH geht im L'Oréal/eBay-Urteil (Urteil vom 12. Juli 2011, C-324/09) sogar davon aus, dass die Haftungsprivilegierung des Art. 14 der e-Commerce-Richtlinie immer dann Anwendung findet, wenn der Diensteanbieter „keine aktive Rolle gespielt hat, die ihm eine Kenntnis der gespeicherten Daten oder eine Kontrolle über sie ermöglicht." Weit davon entfernt, Kenntnis des Plattformbetreibers zu vermuten, obwohl eine vermeintlich rechtswidrige Tätigkeit nicht angezeigt wurde, betont das Gericht darüber hinaus, dass die Haftungsbefreiung selbst dann nicht ausgeschlossen ist, wenn der Plattformbetreiber durchaus benachrichtigt wurde, „da sich Anzeigen vermeintlich rechtswidriger Tätigkeiten oder Informationen als unzureichend genau und substantiiert erweisen können".

Besonders problematisch ist neben der Konstruktion der Regelung jedoch die erwartbare Folge: Hostprovider werden, um sich nicht vor Gericht mit Haftungsfragen herumschlagen müssen, noch weit mehr als heute dazu übergehen, Inhalte in „vorauseilendem Gehorsam" aufgrund des bloßen Verdachts etwaiger Rechtsverletzungen zu entfernen.

Von diesen Einwänden ganz abgesehen, hält der vzbv eine Haftungsverschärfung für Hostprovider ohnehin nicht für sachgerecht. Es ist insbesondere nicht richtig, wie die Begründung darlegt, „dass bei Urheberrechtsverletzungen im Internet ein Vorgehen der betroffenen Inhaber des Rechts auf geistiges Eigentum gegen Diensteanbieter, deren Geschäftsmodelle im Wesentlichen auf Rechtsverletzungen beruht [sic!], vielfach schwierig, wenn nicht unmöglich ist." Nicht nur ist unklar, welche Art von Diensteanbieter im Bereich der Hostprovider hier gemeint ist, nachdem der BGH in seinem Rapidshare-Urteil ausdrücklich klargestellt hat, dass jedenfalls das Geschäftsmodell von Filehostern „nicht von vornherein auf Rechtsverletzungen angelegt" ist. Sondern es ist auch darauf hinzuweisen, dass die Bundesregierung bereits 2008 mit dem „Gesetz zur Verbesserung der Durchsetzung der Rechte des geistigen Eigentums" einen Auskunftsanspruch gegenüber den Providern eingeführt hat, der es Rechteinhabern jederzeit ermöglicht, direkt gegen Rechtsverletzer vorzugehen. Voraussetzung dafür ist ein „gewerbliches Ausmaß" der Rechtsverletzungen, was unstrittig gegeben sein dürfte, sofern es sich um „Geschäftsmodelle" handelt, wie in der Begründung

angegeben. Das erwähnte Gesetz hat sich nicht nur als effektiv im Sinne der Rechteinhaber erwiesen, sondern es ist daraus sogar eine Abmahnindustrie entstanden, bei der Verbraucher mit standardisierten Mahnschreiben und einschüchternden Klageandrohungen zu oftmals ungerechtfertigt überhöhten Zahlungen an die Rechteinhaber gedrängt werden. Jedenfalls hat sich die Bundesregierung aufgrund des anhaltenden Missbrauchs der den „Inhabern des Rechts auf geistiges Eigentum“ eingeräumten Durchsetzungsregeln erst 2013 genötigt gesehen, ein „Gesetz gegen unseriöse Geschäftspraktiken“ zu verabschieden, das leider bis heute weitgehend wirkungslos geblieben ist.

Bekanntlich überziehen die Rechteinhaber heute bereits die Hostprovider mit automatisierten Löschansprüchen, die häufig ebenso automatisiert zu einer Sperrung bzw. Löschung der entsprechenden Inhalte führen. Es ist offenkundig unbefriedigend, dass es zum Teil noch immer keine für beide Seiten befriedigenden Lösungen zur Vergütung der Nutzung urheberrechtlich geschützter Inhalte auf Plattformen gibt. Dieses Problem dadurch lösen zu wollen, dass man die Haftungspflichten nach und nach über die Contentprovider hinaus auf die Hostprovider ausdehnt, hält der vzbv für unsachgemäß. Der vorliegende Regelungsvorschlag ist insofern ein Schritt in die falsche Richtung.

IV. Alternativvorschläge

Der vzbv rät von der Verabschiedung dieses Gesetzentwurfs ab und appelliert an die Bundesregierung und den deutschen Bundestag, unter Berücksichtigung aktueller Entwicklungen sowie der vorliegenden Fachliteratur Alternativvorschläge zu erwägen.

Das Problem der Störerhaftung für Urheberrechtsverletzungen, die von Dritten über offene WLANs begangen werden, ist aus Sicht des vzbv nicht mehr so dringlich, wie es 2010 mit dem BGH-Urteil „Sommer unseres Lebens“ erschien. Seinerzeit war unklar, ob auch Privatleute oder Gewerbetreibende, die ihr WLAN bewusst und absichtlich Dritten zur Verfügung stellen, in dieser Weise haftbar gemacht werden würden. Diese Befürchtung hat sich nicht bestätigt. Im Gegenteil haben Gerichte in jüngster Zeit bei Hotel-WLANs (AG Hamburg, Urteil vom 10.06.2014 – 25b C 431/13) als auch bei WLAN in vermieteten Ferienwohnungen (AG Hamburg, Urteil vom 24.06.2014 – 25b C 924/13) sowie im Zusammenhang mit Freifunk-Netzwerken (AG Charlottenburg, Urteil vom 17.12.2014 – 217 C 121/14) unisono entschieden, dass die Haftungsprivilegierung des § 8 TMG auch in diesen Fällen greift. Zudem hat erst kürzlich das LG München (Beschluss vom 18.09.2014, Az. 7 O

14719/12) die Frage der Haftung bei offenen WLANs dem EuGH vorgelegt. Dabei geht es unter anderem um die Frage einer Differenzierung von privaten und kommerziellen Anbietern, um die Frage der Unterlassungsansprüche sowie um die für Provider im Hinblick auf Urheberrechtsverletzungen zumutbaren Maßnahmen. Zuletzt ist darauf hinzuweisen, dass die Europäische Kommission in Artikel 14 ihres Entwurfs für eine Verordnung über Maßnahmen zum europäischen Binnenmarkt der elektronischen Kommunikation und zur Verwirklichung des vernetzten Kontinents (Telecom Single Market Act) gerade die Frage des Zugangs zu lokalen Funknetzen neu regeln möchte, wobei das erklärte Ziel eine Erleichterung des Zugangs ist und somit dem Ansatz des vorliegenden Gesetzentwurfs diametral entgegensteht, auch wenn diesem die Zugangserleichterung als Ziel zugrunde gelegt wurde.

Vor dem Hintergrund dieser aktuellen Entwicklungen sollte aus Sicht des vzbv anstelle der vorgeschlagenen Einschränkungen der Haftungsbefreiung für Access-Provider allenfalls **eine Klarstellung erfolgen, dass von dem Ausschluss der Verantwortlichkeit nach § 8 TMG gewerbliche und nicht-gewerbliche Betreiber von Funknetzwerken umfasst sind. Zugleich könnte klargestellt werden, dass dieser Ausschluss der Verantwortlichkeit auch Unterlassungsansprüche umfasst.**

Darüber hinaus sollte sichergestellt werden, **dass Klauseln in Endkundenverträgen es Verbrauchern nicht untersagen dürfen, das in ihrem Telekommunikationsvertrag enthaltene Volumen im Rahmen eines nicht-kommerziellen, offenen WLAN-Angebots unbekannten Dritten zur Verfügung zu stellen.** Derartige Klauseln sollten einer AGB-Kontrolle unterworfen werden können. Dies wäre durch einen zusätzlichen Absatz in § 13 TMG zu erreichen. Denn eine Haftungsbefreiung bleibt wirkungslos, wenn Verbraucher von den Telekommunikationsunternehmen daran gehindert werden, ihr WLAN zu öffnen. Kommerzielles WLAN-Sharing, das auf der Nutzung von Netzen der Wettbewerber basiert, könnte hingegen weiterhin als wettbewerbswidrig gelten und als gezielte Behinderung im Sinne von § 4 Nr. 10 UWG angegriffen werden (vergl. OLG Köln, Urteil vom 05.06.2009k, Az. 6 U 223/08).

Auch eine Haftungsverschärfung für Hostprovider ist aus Sicht des vzbv nicht sachgerecht. Dass Hostprovider zum Teil ökonomisch davon profitieren, wenn auf ihre Plattformen urheberrechtlich geschütztes Material widerrechtlich hochgeladen wird, ist unbestritten. Statt einer Verschärfung der Haftungsregelungen sollte hier jedoch eine Klarstellung der dazu ergangenen Rechtsprechung genügen.