Deutscher Bundestag
18. Wahlperiode
Ausschuss für Wirtschaft und Energie

Ausschussdrucksache 18(9)654
15. Dezember 2015

Digitale Gesellschaft e. V.
Sophienstraße 5
D - 10178 Berlin

+49 30 689 16 575

info@digitalegesellschaft.de
www.digitalegesellschaft.de
@digiges

Berlin, den 14. Dezember 2015

# Stellungnahme des Digitale Gesellschaft e.V. zum Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes

Anhörung im Ausschuss für Wirtschaft und Energie des Deutschen Bundestages,

16. Dezember 2015

## Inhalt:

## 1. Zusammenfassung

Mit der Herstellung von Rechtssicherheit beim Betrieb offener WLAN-Hotspots verfolgt der Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (2. TMGÄndG) ein nach Ansicht des Digitale Gesellschaft e.V. begrüßenswertes gesetzgeberisches Ziel. Die derzeit vorgesehene Regelung ist der Erreichung dieses Ziels jedoch nicht förderlich, sondern im Gegenteil sogar abträglich. Tatsächlich verhindert der Entwurf in der gegenwärtigen Fassung den Betrieb offener Funknetze und schreibt die aktuell bestehende Rechtsunsicherheit fest. Diese Fehlwirkung wird allein durch den vorgesehenen § 8 Abs. 4 und die darin geforderten, unscharf formulierten „zumutbaren Maßnahmen" verursacht.

Für bereits im Ansatz verfehlt halten wir zudem die geplante Verschärfung der Host-Providerhaftung. Damit würden insbesondere für den Betrieb von Cloud-Computing-Diensten neue Rechtsunsicherheiten geschaffen, was zu einem deutlichen Rückgang der Investitionsbereitschaft bei derartigen Geschäftsmodellen beitragen könnte. Die im Entwurf enthaltenen Kriterien für die Definition des „gefahrgeneigten Dienstes" sind darüber hinaus schlicht unpraktikabel.

Beide angesprochenen Änderungen werfen in der vorliegenden Fassung überdies europarechtliche Probleme auf.

**Im Ergebnis empfehlen wir daher, den unter Nr. 3 vorgesehenen § 8 Abs. 4 TMG sowie die komplette Nr. 4 zu streichen. Anstelle des § 8 Abs. 4 TMG könnte eine gesetzgeberische Evaluierung zur Häufigkeit der über offene Drahtlosnetze begangenen Rechtsverletzungen aufgenommen werden. Im Übrigen halten wir den Entwurf für zustimmungswürdig.**

## 2. Vorbemerkungen zur WLAN-Störerhaftung

### 2.1 Potenziale und Bestand offener Funknetzzugänge

Die rasanten Fortschritte im Bereich der Informationstechnologie bieten ein breites Spektrum neuer Möglichkeiten, gerade auch für demokratische Teilhabe, zivilgesellschaftlichen Diskurs, lebenslanges Lernen und innovative Geschäftsmodelle. Wesentliche Voraussetzung einer funktionsfähigen Informationsgesellschaft ist jedoch ein möglichst leichter und kostengünstiger Zugang zum Internet, unabhängig vom konkreten Aufenthaltsort.

Über ortsgebundene Breitband-Anschlüsse und mobile Datenkommunikation stehen zwar relativ leicht zugängliche und leistungsfähige Wege für einen Zugang zum Internet zur Verfügung. Gerade mobile Netzzugänge sind jedoch in der Regel volumenbeschränkt, so dass der Datenfluss nach Ausschöpfen des jeweiligen Kontingents auf äußerst niedrige Geschwindigkeiten gedrosselt wird. Datenintensive

Dienste wie Videostreaming sind mobil daher kaum bis gar nicht nutzbar. Viele Netzbetreiber verbieten in ihren AGB außerdem die Verwendung bestimmter Online-Dienste wie etwa Voice-over-IP (z.B. Skype), Instant Messaging (z.B. Threema oder WhatsApp) oder Virtual Private Networks (VPN). Schließlich kann die Nutzung mobiler Datenkommunikation in Deutschland aufgrund der anfallenden Roaming-Gebühren insbesondere für Touristen verhältnismäßig teuer ausfallen, so dass sie im Zweifel nur zögerlich darauf zurückgreifen werden.

Diese Beschränkungen und Nachteile der mobilen Datennutzung lassen sich umgehen, indem der Zugang zum Internet über offene Funknetze, auch WLAN-Hotspots genannt, erfolgt. Hier ist der Kreis der verfügbaren Anwendungen und Online-Dienste in der Regel nicht eingeschränkt und auch die Bandbreite wird für gewöhnlich nicht nach Erreichen einer Volumengrenze gedrosselt. In einer zunehmend digitalisierten Gesellschaft kann die flächendeckende Versorgung mit leistungsstarken Internetzugängen daher durchaus als Teil der öffentlichen Daseinsvorsorge begriffen werden. Naturgemäß sind die staatlichen Möglichkeiten begrenzt, etwa durch den Aufbau von kostenfreien „Bürgernetzen" einen leichteren Zugang zum Netz zu schaffen. Allerdings werden in der Bundesrepublik mehrere Millionen privater und öffentlicher Funknetze (sog. WLAN) betrieben, die grundsätzlich von den Menschen in der näheren Umgebung für den Zugang zum Internet genutzt werden könnten. Damit wäre im Grundsatz bereits heute jedenfalls in dichter besiedelten Gebieten nahezu flächendeckend ein allgemeiner Internetzugang verfügbar.

Gleichwohl haben freie WLAN-Hotspots und offene Funknetze in Deutschland noch immer Seltenheitswert. Während in den USA gut fünf, im Vereinigten Königreich über 28 und in Südkorea mehr als 37 offene WLAN-Hotspots auf 10.000 Einwohner kommen, sind es in Deutschland noch nicht einmal zwei.[1] Die Gründe dafür liegen weder in einer zu geringen Nachfrage seitens der Nutzerinnen und Nutzer, noch in einem mangelnden Interesse bei potenziellen Anbietern, noch in Gefahren für Datensicherheit und Datenschutz bei unverschlüsselten Netzwerken. Die Mangelsituation wird vielmehr allein durch die gegenwärtige Rechtslage und die damit verbundenen Haftungsrisiken beim Betrieb offener Drahtloszugänge zum Internet verursacht.

### 2.2 Unklare Rechtslage beim Betrieb offener Funknetze

Gemäß § 8 Abs. 1 TMG sind Anbieter, die lediglich Informationen durch ein Kommunikationsnetz durchleiten (sog. Zugangs- oder Access-Provider), grundsätzlich nicht für die durchgeleiteten Informationen verantwortlich (sog. Providerprivileg). Trotz dieser eigentlich deutlich gefassten Regelung ist bislang nicht abschließend geklärt, für welche Anbieter die Haftungsfreistellung gilt und unter welchen Voraussetzungen sie greift. Während die Rechtsprechung die Privilegierung bei gewerblichen

1 https://www.eco.de/wp-content/blogs.dir/eco-microresearch_verbreitung-und-nutzung-von-wlan.pdf

Anbietern, deren Geschäftsschwerpunkt in der Vermarktung von Internetzugängen liegt („klassische" Provider wie Deutsche Telekom, Vodafone, Unitymedia etc), ohne Weiteres für anwendbar hält, bestehen Unsicherheiten vor allem bei gewerblichen, nichtkommerziellen und rein privaten „Nebenbei-Providern". Darunter fallen etwa Hotels und Cafés, die ihren Gästen WLAN-Zugänge anbieten, aber auch Schulen, Jugendeinrichtungen, Initiativen wie die „Freifunker" sowie Privatleute, die ihre Drahtlosnetze nicht mit Verschlüsselung und Passwort versehen. Für diese Gruppe von Betreibern nimmt die höchstrichterliche Rechtsprechung eine verschuldensunabhängige Störerhaftung für rechtswidrige Handlungen Dritter an, die über ein nicht ausreichend gegen Missbrauch gesichertes Netzwerk begangen werden (vgl. BGH, Urteil vom 12. Mai 2010, I ZR 121/08 - „Sommer unseres Lebens").

Um diesem Haftungsrisiko zu entgehen, müssen die Betreiber ihre Netze nach Ansicht der Rechtsprechung gegen Missbrauch schützen, indem sie ausreichend sichere Passworte verwenden und ihre Router verschlüsseln. Ob es in diesem Zusammenhang genügt, für sämtliche Nutzerinnen und Nutzer dasselbe Passwort zu verwenden, oder ob in jedem Einzelfall ein individuelles Passwort vergeben werden muss, ist dabei ebenso ungeklärt wie die Frage, ob und gegebenfalls wie häufig die Passwörter geändert werden müssen.

Streng betrachtet betrifft diese Rechtsprechung allerdings nicht den Fall, in dem die vorgenannten Betreiber ihr Netzwerk bewusst und vorsätzlich mit dem expliziten Ziel öffnen, der Allgemeinheit Zugang zum Internet zu vermitteln. Vor dem Hintergrund der BGH-Rechtsprechung mag es in einer solchen Konstellation zwar naheliegen, eine Haftung im Wege eines Erst-recht-Schlusses anzunehmen; demgegenüber hat jedoch das Amtsgericht Charlottenburg (vgl. Beschluss vom 17. Dezember 2014, 217 C 121/14) entschieden, dass sich die Betreiber eines öffentlich zugänglichen WLAN-Netzwerks sehr wohl auf das Providerprivileg berufen können und die Störerhaftung bei ihnen deshalb nicht greift. Mangels einheitlicher Rechtsprechung ist ein Haftungsrisiko beim Betrieb offener Funknetze daher im Ergebnis nicht auszuschließen. Diese Unsicherheit führt dazu, dass gerade „Nebenbei-Provider" ihre Drahtlosnetze regelmäßig verschlüsseln und auf diese Weise der kostenfreien Mitnutzung durch andere Menschen entziehen.

Die Störerhaftung erstreckt sich dabei zwar nur auf Unterlassungsansprüche, jedoch können auch diese kostenpflichtig abgemahnt werden. Besondere Gefahren gehen sind in diesem Zusammenhang von Abmahnungen wegen vermeintlicher Urheberrechtsverletzungen aus, deren Kosten durchaus vierstellige Beträge erreichen. Die vom Gesetzgeber in § 97a Abs. 3 UrhG vorgesehene Begrenzung der Anwaltskosten für eine erste Abmahnung auf einen Gegenstandswert von 1.000€, mithin Gebühren von rund 150€, bleibt in der Praxis weitgehend wirkungslos: sie gilt nur für natürliche Personen, die weder

gewerblich noch in Ausübung einer selbständigen beruflichen Tätigkeit handeln. In Wiederholungsfällen und bei Unbilligkeit greift die Beschränkung ebenfalls nicht.

## 3. Zum Entwurf des 2. TMGÄndG

### 3.1 Nr. 3; § 8 Abs. 3 TMG

Die in § 8 Abs. 3 TMG vorgesehene gesetzliche Klarstellung, wonach sich auch Betreiber von Drahtlosnetzwerken auf das Providerprivileg des § 8 Abs. 1 TMG berufen können, halten wir für überfällig und befürworten sie daher ausdrücklich.

### 3.2 Nr. 3; § 8 Abs. 4 TMG

Abzulehnen ist hingegen die in § 8 Abs. 4 TMG vorgesehene Regelung, mit der die Haftungsprivilegierung für WLAN-Betreiber von der Ergreifung „zumutbarer Maßnahmen" abhängig gemacht wird.

#### 3.2.1 Verfehlung des gesetzgeberischen Ziels

Die Regelung des § 8 Abs. 4 TMG hat zunächst zur Folge, dass das von der Großen Koalition selbst gesteckte gesetzgeberische Ziel der TMG-Änderung, nämlich die Schaffung eines sicheren Rechtsrahmens für den Betrieb offener Funknetze, verfehlt wird.

Zum Thema WLAN-Störerhaftung heißt es in der Koalitionsvereinbarung von CDU, CSU und SPD auf Seite 37: *„Wir wollen, dass in deutschen Städten mobiles Internet über WLAN für jeden verfügbar ist. Wir werden die gesetzlichen Grundlagen für die Nutzung dieser offenen Netze und deren Anbieter schaffen."*

Offene Netze zeichnen sich gerade dadurch aus, dass sie keinerlei Zugangshürden aufweisen und der Kreis der Zugriffsberechtigten in keiner Weise beschränkt ist. Der Zugriff auf offene Netze ist vielmehr stets ohne Weiteres möglich und nicht von der Erfüllung bestimmter Vorbedingungen abhängig. Demgegenüber verlangt § 8 Abs. 4 S. 1 TMG von den Betreibern, dass sie „zumutbare Maßnahmen ergriffen haben, um eine Rechtsverletzung durch Nutzer zu verhindern." Wie aus dem folgenden Satz hervorgeht, sollen solche Maßnahmen insbesondere darin bestehen, das Drahtlosnetzwerk gegen unberechtigte Zugriffe zu sichern und den Zugang zum Internet nur solchen Nutzern zu gewähren, die zuvor erklärt haben, in diesem Rahmen keine Rechtsverletzungen zu begehen.

Durch die beiden in § 8 Abs. 4 S. 2 TMG beispielhaft aufgeführten Maßnahmen werden Zugangshürden aufgebaut, die als solche der soeben skizzierten Kernidee eines offenen Netzes diametral widersprechen. In einem offenen Netz kann es darüber hinaus schon begrifflich keine unberechtigten Zugriffe geben, da der Kreis der Zugriffsberechtigten a priori gerade nicht eingeschränkt ist.

### 3.2.2 Festschreibung der Rechtsunsicherheit

Mit der Regelung des § 8 Abs. 4 TMG wird zudem das aufgrund der unvollständigen und uneinheitlichen Rechtsprechung bestehende Haftungsrisiko gesetzlich festgeschrieben.

Durch der Verwendung unbestimmter Rechtsbegriffe wie „zumutbare Maßnahmen" und „angemessene Sicherungsmaßnahmen gegen unberechtigte Zugriffe" ist für die Betreiber von Drahtlosnetzen nach wie vor unklar, was sie genau tun müssen, um der WLAN-Störerhaftung zu entgehen. Zwar führt die Entwurfsbegründung in diesem Zusammenhang beispielhaft die Verschlüsselung des Routers oder eine Registrierung der Nutzer an; diese Ausführungen sind jedoch nicht Teil des eigentlichen Gesetzestextes und insoweit auch nicht verbindlich. Sie geben daher lediglich eine Ansicht des Entwurfsverfassers wieder. Wie § 8 Abs. 4 TMG genau auszulegen und anzuwenden ist, müsste wiederum erst durch die Rechtsprechung geklärt werden.

Im Ergebnis verschärft § 8 Abs. 4 TMG sogar die gegenwärtig unklare haftungsrechtliche Lage beim Betrieb offener Funknetze. Anders als nach dem oben dargelegten gegenwärtigen Stand der Rechtsprechung wird mit § 8 Abs. 4 TMG die Pflicht zur Ergreifung „zumutbarer Maßnahmen" unterschiedslos für sämtliche Betreiber von Drahtlosnetzen kodifiziert.

### 3.2.3 Häufigkeit von Rechtsverletzungen, Tauglichkeit der „zumutbaren Maßnahmen"

Die in § 8 Abs. 4 S. 2 TMG nur unscharf umrissenen Maßnahmen sind zur Verhinderung von Rechtsverletzungen durch die Nutzer eines Drahtlosnetzwerk des Weiteren auch gänzlich ungeeignet.

Fraglich ist zunächst, inwieweit offene Netzzugänge überhaupt zu Rechtsverletzungen im Internet beitragen. Die Entwurfsbegründung behauptet lediglich allgemein, dass mit der Ermöglichung des Zugangs zum Internet auch „eine potenzielle Gefahrenquelle zur Begehung rechtswidriger Taten" geschaffen werde (vgl. S. 13). Das ist in dieser pauschalen Form jedoch nicht richtig. Wenn schon die bloße Eröffnung des Zugangs zu einer Kommunikationsinfrastruktur mit der Schaffung einer Gefahrenquelle gleichzusetzen wäre, so müsste dies genauso gut etwa für Telefonzellen oder Briefkästen gelten. Abgesehen davon entbehrt eine solche Behauptung auch einer belastbaren empirischen Grundlage. Die verfügbaren Fakten legen sogar das Gegenteil nahe. So äußerte beispielsweise der Hotspot-Betreiber Kabel Deutschland/Vodafone im Rahmen der vom Bundesministerium für Wirtschaft und Energie zum 2. TMGÄndG durchgeführten Anhörung, dass an seinen frei zugänglichen Hotspots keine Probleme mit Urheberrechtsverletzungen, z.B. durch illegales Filesharing zu beobachten seien.[2] Auch die Medienanstalt Berlin-Brandenburg konnte bei ihrem seit 2012

2 http://www.bmwi.de/BMWi/Redaktion/PDF/Stellungnahmen/Stellungnahmen-WLAN/vodafone,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

laufenden Public Wi-Fi Projekt keinen Missbrauch der Hotspots für Urheberrechtsverletzungen feststellen.[3]

### 3.2.3.1 Angemessene Sicherungsmaßnahmen

Unabhängig davon stellen die in § 8 Abs. 4 S. 2 TMG aufgeführten Maßnahmen auch keine probaten Mittel zur Verhinderung von Rechtsverletzungen im Internet dar. Sicherungsmaßnahmen gegen unberechtigten Zugriff, wie etwa die Verschlüsselung des Routers und/oder die Verwendung eines Passworts, bewirken lediglich, dass Nutzerinnen und Nutzer diese Informationen benötigen, um Zugang zum Internet zu erhalten. Auf das, was sie anschließend über diesen Zugang im Internet tun, haben die Sicherungsmaßnahmen keinerlei Einfluss.

Anders als in der Entwurfsbegründung angedeutet (vgl. S. 13), erhöhen Verschlüsselung und Passwortsicherung auch nicht die Netzwerksicherheit. Handelsübliche Router erlauben es dem Betreiber schon heute, parallel zu einem öffentlichen auch ein privates Netz aufzuspannen und dieses komplett gegenüber dem öffentlichen abzuschotten. Es bedarf daher für die Sicherheit des betreibereigenen Netzes keiner Verschlüsselung oder Passwortsicherung.

Derartige Maßnahmen würden im Übrigen nicht zu einer Verbesserung der Datensicherheit für die Nutzerinnen und Nutzer beitragen. Dies würde vielmehr dadurch gewährleistet, dass Nutzerinnen und Nutzer beim Surfen kryptographisch gesicherte Protokolle wie https und beim Versenden von Mails Verschlüsselungsdienste wie PGP verwenden. Die Entwurfsbegründung verwechselt insoweit die Verschlüsselung des Funknetzes (also der Infrastruktur) mit der Verschlüsselung des über dieses Funknetz laufenden Datenverkehrs (also den darüber transportierten Inhalten).

### 3.2.3.2 Rechtstreueerklärung

Auch die in § 8 Abs. 4 S. 2 Nr. 2 TMG angeführte Rechtstreueerklärung ist zur Verhinderung von Rechtsverletzungen im Internet untauglich. Nutzerinnen und Nutzer würden mit der Rechtstreueerklärung lediglich eine Selbstverständlichkeit bestätigen, nämlich sich an geltendes Recht zu halten. Auf ihr anschließendes Verhalten im Internet hätte die Erklärung hingegen keinen Einfluss.

Insbesondere ist auch eine disziplinierende oder einschüchternde Wirkung auf die Nutzerinnen und Nutzer nicht zu erwarten. Die Abgabe der Rechtstreueerklärung würde sich darin erschöpfen, auf einer Vorschaltseite ein Häkchen zu setzen oder eine Schaltfläche anzuklicken. Wer darin ein wirksames Mittel zur Bekämpfung von Rechtsverletzungen im Internet erblickt, muss konsequenterweise auch die Altersabfrage auf Videoportalen mit pornographischen Inhalten für eine effektive Maßnahme des

3 http://www.mabb.de/files/content/document/Stellungnahmen/mabb_Stellungnahme_BMWi_TMGAendG.pdf

Jugendschutzes und das Wegklicken von AGBen bei Social-Media-Plattformen für eine taugliche Vorkehrung des Verbraucherschutzes halten. Tatsächlich entbehrt die Annahme, dass auf diese Weise irgendein verhaltensbeeinflussender Effekt erzielt werden könnte, einer sachlichen Grundlage. Sie erweist sich damit als bloßes realitätsfernes Wunschdenken.

### 3.2.4 Mangelnde Praktikabilität der „zumutbaren Maßnahmen"

Die in § 8 Abs. 4 S. 2 TMG aufgeführten Maßnahmen wären für viele potenzielle WLAN-Betreiber auch nur schwer umsetzbar. Während Verschlüsselung und Passwortsicherung heute zu den Standardfunktionen eines Routers gehören und auch von Laien technisch gut bewältigt werden können, stellt insbesondere das Einrichten einer Vorschaltseite eine weitaus höhere Hürde dar.

Eine Vorschaltseite mit Rechtstreueerklärung ist bei den meisten Routermodellen noch nicht in die Firmware integriert. Zwar enthalten offene Firmwares wie OpenWRT grundsätzlich solche Funktionen, ihre Einrichtung erfordert jedoch fortgeschrittene technische Kenntnisse, die bei Weitem nicht alle potenziellen Funknetzbetreiber mitbringen. Sie sind daher darauf angewiesen, entweder diese Dienstleistung teuer einzukaufen oder auf das Angebot offener WLAN-Zugänge zu verzichten.

### 3.2.5 Unvereinbarkeit mit EU-Recht

§ 8 Abs. 4 TMG verstößt zudem gegen Vorgaben des EU-Rechts, namentlich Art. 12 E-Commerce-Richtlinie und Art. 16 EU-Grundrechte-Charta.

#### 3.2.5.1 Verstoß gegen Artikel 12 E-Commerce-Richtlinie

§ 8 Abs. 4 TMG ist nicht mit Art. 12 Abs. 1 der E-Commerce-Richtlinie vereinbar. Art. 12 Abs. 1 E-Commerce-Richtlinie zählt abschließend die Bedingungen auf, unter denen Access-Provider nicht für die über ihr Netzwerk übermittelten Informationen verantwortlich sind. Demgegenüber postuliert § 8 Abs. 4 TMG speziell für Diensteanbieter von Drahtlosnetzwerken weitere Voraussetzungen für die Haftungsfreistellung („zumutbare Maßnahmen [...], um eine Rechtsverletzung durch Nutzer zu verhindern."). Bereits damit überschreitet die geplante Regelung des § 8 Abs. 4 TMG den durch Art. 12 Abs. 1 E-Commerce-Richtlinie gesteckten Regulierungsrahmen.

Hinzu kommt, dass § 8 Abs. 4 Satz 1 TMG mit dem unbestimmten Rechtsbegriff der „zumutbaren Maßnahmen" keine klare Eingrenzung der Voraussetzungen vornimmt, unter denen ein Diensteanbieter sich auf die Haftungsfreistellung berufen kann. Auch der nachfolgende Satz, in dem beispielhaft („insbesondere") zwei „zumutbare Maßnahmen" benannt werden, gibt keine erschöpfende Antwort auf die Frage, welche Bedingungen ein Diensteanbieter zu erfüllen hat, um in den Genuss der Privilegierung zu kommen. Entgegen der Vorgabe von Art. 12 Abs. 1 E-Commerce-Richtlinie stellt § 8 Abs. 4 TMG daher

keineswegs sicher, dass der Diensteanbieter nicht für die übermittelten Informationen verantwortlich ist. Vielmehr entsteht durch die unvollständige Regelung eine neue Rechtsunsicherheit für Diensteanbieter von Drahtlosnetzwerken.

#### 3.2.5.2 Verstoß gegen Art. 16 EU-Grundrechte-Charta

Die Regelung des § 8 Abs. 4 TMG verstößt des Weiteren gegen das EU-Grundrecht auf unternehmerische Freiheit aus Art. 16 EU-Grundrechte-Charta.

Das Recht auf unternehmerische Freiheit umfasst unter anderem das Recht jedes Unternehmens, in den Grenzen seiner Verantwortlichkeit für seine eigenen Handlungen frei über seine wirtschaftlichen, technischen und finanziellen Ressourcen verfügen zu können. § 8 Abs. 4 TMG verlangt von einem Unternehmen, das als Diensteanbieter im Sinne der Vorschrift agiert, einen Teil seiner Ressourcen für die geforderten „zumutbaren Maßnahmen" einzusetzen. Daher verkürzt § 8 Abs. 4 TMG die in Art. 16 EU-Grundrechte-Charta garantierte unternehmerische Freiheit.

Wie der Wortlaut des § 8 Abs. 4 Satz 1 TMG erkennen lässt, sollen die „zumutbaren Maßnahmen" dazu dienen, Rechtsverletzungen durch Nutzer zu verhindern. In Betracht kommen dabei etwa Verletzungen des Urheberrechts, welches als Teil des geistigen Eigentumsrechts dem Schutz des Art. 17 Abs. 2 EU-Grundrechte-Charta unterliegt. Der Europäische Gerichtshof hat bereits entschieden, dass es im Fall mehrerer kollidierender Grundrechte Sache der Mitgliedstaaten ist, bei der Umsetzung einer Richtlinie (hier: E-Commerce-Richtlinie) darauf zu achten, dass sie sich auf eine Auslegung dieser Richtlinie stützen, die es ihnen erlaubt, ein angemessenes Gleichgewicht zwischen den durch die Unionsrechtsordnung geschützten anwendbaren Grundrechten sicherzustellen (vgl. in diesem Sinne Urteil vom 29. Januar 2008, Promusicae, C-275/06, Slg. 2008, I-271, Rn. 68). Ordnet ein Mitgliedstaat zu diesem Zweck bestimmte Maßnahmen an, so müssen diese nach Ansicht des EuGH „hinreichend wirksam sein, um einen wirkungsvollen Schutz des betreffenden Grundrechts 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" (vgl. Urt. v. 27. 03. 2014, C-314/12, Rn 62).

§ 8 Abs. 4 TMG erfüllt diese Voraussetzungen nicht. Die in § 8 Abs. 4 Satz 2 TMG beispielhaft aufgeführten Maßnahmen sind offensichtlich ungeeignet, Urheberrechtsverletzungen oder andere Rechtsverstöße durch die Nutzer eines Diensteanbieters im Sinne der Vorschrift zu verhindern. Weder die dort vorgesehenen Sicherungsmaßnahmen gegen unberechtigten Zugriff noch die Rechtstreueerklärung verhindern oder erschweren für die Nutzer unerlaubte Zugriffe auf Schutzgegenstände. Faktisch

bedeuten diese Maßnahmen nämlich nur, dass die Nutzer sich mit einem öffentlich ausliegenden Passwort einloggen und durch einem bloßen weiteren Mausklick eine Rechtstreueerklärung abgeben müssen, um Zugang zu dem Drahtlosnetzwerk zu erhalten. Auf das, was die Nutzer anschließend über diesen Zugang im Netz machen, haben die Maßnahmen keinerlei Einfluss.

### 3.2.6 Empfehlung: Streichung des § 8 Abs. 4 TMG und Evaluation

Wir empfehlen daher, den § 8 Abs. 4 TMG ersatzlos zu streichen. Den nach unserer Ansicht unbegründeten, aber dennoch in Teilen vorhandenen Befürchtungen einer Zunahme von Rechtsverletzungen über offene Drahtlosnetzzugänge kann im Wege einer Evaluation der Auswirkungen nach Ablauf eines Jahres seit Inkrafttreten des Gesetzes begegnet werden.

### 3.3 zu Nr. 4; § 10 TMG

Die in § 10 TMG vorgesehene Verschärfung der Host-Providerhaftung ist aus unserer Sicht ebenfalls abzulehnen. Die Änderung würde zu erheblichen Rechtsunsicherheiten führen, die ihrerseits Schwierigkeiten bei der Anwendung des Gesetzes sowie Investitionshemmnisse zur Folge hätten. Darüber hinaus ist die Verschärfung in der vorliegenden Fassung nicht mit dem Europarecht vereinbar.

### 3.3.1 Rechtsunsicherheit

Nach § 10 Abs. 2 S. 1 TMG hat das Vorliegen eines gefahrgeneigten Dienstes zur Folge, dass die für den rechtssicheren Betrieb von Host-Providerangeboten essenzielle Haftungsprivilegierung entfällt. Wann ein gefahrgeneigter Dienst vorliegt, wird in § 10 Abs. 2 S, 2 TMG jedoch nicht abschließend, sondern lediglich anhand von Regelbeispielen definiert. Bereits an dieser Stelle beginnen für einen Diensteanbieter die rechtlichen Unwägbarkeiten.

Diese Unsicherheit wird durch die konkrete Formulierung der Regelbeispiele weiter vertieft. So ist insbesondere das unter § 10 Abs. 2 S. 2 Nr. 1 TMG aufgeführte Kriterium, dass „die Speicherung oder Verwendung der weit überwiegenden Zahl der gespeicherten Informationen rechtswidrig erfolgt", nur schwer subsumierbar. Für einen Host-Provider dürfte in der Regel kaum festzustellen sein, ob Informationen bei ihm rechtswidrig gespeichert sind. Selbst urheberrechtlich geschützte Werke dürfen bei einem Host-Provider gespeichert werden, solange der Uploader sie rechtmäßig erworben hat und sie nicht öffentlich zugänglich macht (etwa durch das öffentliche Verbreiten eines Download-Links). Unklar ist des Weiteren, ab welchem Prozentsatz die Grenze zur „weit überwiegenden Zahl der gespeicherten Inhalte" überschritten wird.

### 3.3.2. Überzogene Sperrpolitik und Investitionshemmnis

Diese Rechtsunsicherheiten könnten Host-Provider zu einer überzogenen Lösch- und Sperrpolitik veranlassen, durch die auch rechtmäßige Inhalte in Mitleidenschaft gezogen werden könnten. Um nicht als „gefahrgeneigter Dienst" zu gelten, könnten Host-Provider dazu übergehen, sämtliche Inhalte, die nicht evident rechtmäßig sind, zu beseitigen. Dies hätte empfindliche Einschränkungen bei der Nutzbarkeit von Host-Providerdiensten zur Folge.

Ebenso negativ dürfte sich eine derart unsichere Rechtslage auch auf die Investitionsbereitschaft bei Host-Providerdiensten auswirken. Da unter den Bedingungen des § 10 Abs. 2 TMG ein dauerhafter Betrieb eines Host-Providers nicht gewährleistet werden kann, ist ein massives Abfließen von Investitionsmitteln in diesem Bereich zu erwarten.

Beide beschriebenen Effekte wären vor allem deshalb verheerend, weil sie nur im Geltungsbereich des TMG, also in Deutschland, auftreten würden. Die aus urheberrechtlicher Sicht problematischen One-Click-Hoster, über die heute ein Großteil des illegalen Filesharings abgewickelt wird, befinden sich zumeist im Ausland. Gerade sie würden von der Haftungsverschärfung folglich nicht erfasst. Host-Provider sind jedoch auch Dienste wie Youtube, Wikipedia, Soundcloud, Dropbox sowie der gesamte Bereich des Cloud-Computings. Mit der Haftungsverschärfung würde gerade in diesem zukunftsträchtigen Marktsegment ein massiver Wettbewerbsnachteil für Start-Ups aus Deutschland geschaffen. Die Verschärfung würde faktisch bedeuten, dass Deutschland sich von der internationalen Entwicklung in diesem Bereich komplett abkoppeln würde.

### 3.3.3 Unvereinbarkeit mit EU-Recht

Auch die vorgesehene Änderung des § 10 TMG verstößt gegen EU-Recht.

#### 3.3.3.1 Verstoß gegen Art. 14 E-Commerce-Richtlinie

Insbesondere die Vermutungsregel des § 10.2 Satz 1 TMG-E ist mit Art. 14 E-Commerce-Richtlinie nicht vereinbar. Art. 14 Abs. 1 lit. a E-Commerce-Richtlinie stellt für die Haftungsfreistellung des Host-Providers allein auf dessen „tatsächliche Kenntnis von der rechtswidrigen Tätigkeit oder Information" ab. Für Schadensersatzansprüche greift die Privilegierung, wenn der Diensteanbieter sich (tatsächlich) „keiner Tatsachen oder Umstände bewusst" ist, „aus denen die rechtswidrige Tätigkeit oder Information offensichtlich wird". Die E-Commerce-Richtlinie verlangt demnach ein positives Vorliegen der Kenntnis bzw des Bewusstseins. § 10 Abs. 2 S. 1 TMG hingegen ersetzt dieses Erfordernis durch eine bloße gesetzliche Vermutung. Damit überschreitet die Regelung den durch die E-Commerce-Richtlinie gezogenen Rahmen.

#### 3.3.3.2 Verstoß gegen Art. 15 E-Commerce-Richtlinie

Auch die Ausfüllung des Vermutungstatbestandes in § 10 Abs. 2 S. 2 TMG begegnet rechtlichen Bedenken. So verstößt § 10 Abs. 2 S. 2 Nr. 1 TMG gegen Art. 15 Abs. 1 E-Commerce-Richtlinie.

Nach § 10 Abs. 2 S. 2 Nr. 1 TMG greift die gesetzliche Vermutung des Absatz 1 bereits dann ein, wenn „die Speicherung oder Verwendung der weit überwiegenden Zahl der Informationen rechtswidrig erfolgt". Ein Host-Provider wäre daher gezwungen, sämtliche bei ihm gespeicherten Informationen proaktiv nach Rechtsverstößen zu durchsuchen und nach Umständen zu forschen, die auf eine rechtswidrige Speicherung oder Verwendung hinweisen. Genau dies verbietet jedoch Art. 15 Abs. 1 E-Commerce-Richtlinie. Auch an dieser Stelle verstoßen die vorgesehenen Änderungen des § 10 TMG daher gegen das EU-Recht.