Deutscher Bundestag
18. Wahlperiode
Ausschuss für Wirtschaft und Energie

Ausschussdrucksache 18(9)653
15. Dezember 2015

Stellungnahme zum Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Drucksache 18/6745)

1 Einleitung

Die hotsplots GmbH arbeitet seit zehn Jahren hart daran, in Deutschland die Versorgung mit WLAN-Hotspots zu verbessern. Unsere derzeit 37 Mitarbeiter und über 300 Partnerfirmen, die Kunden vor Ort technisch betreuen, nehmen im Mittel alle drei Stunden einen neuen Hotspot-Standort in Betrieb. Je nach Größe spannen diese Standorte teils mit einem, teils mit mehr als 1.000 Access Points WLAN-Netze auf, die kostenfrei oder kostenpflichtig, aber immer ohne Vertragsbindung nutzbar sind.

Nach unserer Einschätzung sind wir sehr erfolgreich damit, WLAN in diesem Land voranzubringen. Da macht es uns immer wieder betroffen, zu lesen, dass wir im internationalen Vergleich die rote Laterne tragen würden. In Zi. 2 werden wir aufzeigen, dass die Situation in Deutschland keinesfalls schlecht und damit der Anlass für die Gesetzesänderung hinfällig ist.

Das wird auch in den Medien leider häufig falsch dargestellt, wie man anschaulich sieht, wenn man auf google nach „wlan anbieten“ sucht.[1] Dann erhält man auf der ersten Seite Links zu professionellen Angeboten für einen rechtssicheren, komfortablen Betrieb lokaler WLAN-Hotspots von uns und 13 unserer Wettbewerber – doch ganz unten steht:
„Warum es in Deutschland kein freies WLAN gibt – Die Welt“

Wenn man es schaffen könnte, die Berichterstattung in korrektere, positivere Bahnen zu lenken, dann könnte man vielleicht mehr für die sinnvolle Ausbreitung von WLAN erreichen, als mit dem vorliegenden Gesetzesentwurf. Denn dieser ist jedenfalls nicht dazu geeignet, die Anzahl an WLAN-Hotspots in Deutschland quantitativ und qualitativ zu steigern, siehe Zi. 2.2.1.

Die folgenden Ausführungen dienen der kritischen Betrachtung des Änderungsentwurfes zum § 8 TMG.

2 Zu „A Problem“: Die Lage in Deutschland ist viel besser als dargestellt

Die Beschreibung des Problems stimmt nicht mit der Realität überein. Die Argumentation mit den zugrunde liegenden Zahlen ist bei näherer Betrachtung nicht aufrecht zu erhalten.

2.1 These 1: In Deutschland gibt es viel weniger WLAN-Hotspots als im Ausland.

Der Gesetzesentwurf führt als Problem an, dass die Verfügbarkeit von WLAN in Hotels und zunehmend auch in Innenstädten, Cafés, Flughäfen und Wartebereichen im Allgemeinen in Deutschland wesentlich geringer als in vielen anderen Ländern sei und beruft sich dabei auf eine Erhebung des eco-Verbandes vom Dezember 2014 (richtig: November 2014).

Kaum jemandem scheint aufgefallen zu sein, dass in dieser Erhebung für den internationalen Vergleich 98,49 % der Hotspots in Deutschland nicht berücksichtigt wurden, weil nur „Vollkommen freie Hotspots, die ohne Registrierung oder Identifikation genutzt werden können“ in den internationalen Vergleich einbezogen wurden.

Zwar stellt der eco-Verband dies in seiner Studie klar und transparent dar, in den Medien und dem vorliegenden Gesetzesentwurf wird dieser wichtige Umstand jedoch nicht berücksichtigt. So wird auf der Website des Bundesministeriums für Wirtschaft und Energie, das federführend für diesen Gesetzesentwurf ist, die Hotspot-Anzahl

1 Stand 21.11.2015

hotsplots GmbH, Rotherstr. 22, 10245 Berlin – Website: www.hotsplots.de – E-Mail: info@hotsplots.de
Geschäftsführende Gesellschafter: Dr. Ulrich Meier, Dr. Jörg Ontrup – USt-IdNr.: DE237345081 – Register: Amtsgericht Charlottenburg HRB 93460B

in Deutschland um den Faktor 60 zu niedrig angegeben, indem dort beim Zitieren der Zahlen aus der Erhebung des eco-Verbandes, auf den Zusatz „Freie“ verzichtet wurde.[2]

Berücksichtigt man die „ständig wachsenden Marktanteile“ (Zitat Bundesnetzagentur[3]) von WLAN, so liegt die gesamte Anzahl der WLAN-Hotspots in Deutschland, unter der Annahme, dass sich diese proportional zur Anzahl der Hotspots von HOTSPLOTS entwickelt (+80% seit Unterzeichnung des Koalitionsvertrages vor 24 Monaten), Ende 2016 sogar um den Faktor 100 höher als sie derzeit auf der Internetseite des BMWi angegeben ist.
Das bedeutet, dass in Deutschland aktuell nicht 1,87 sondern eher 187 WLAN-Hotspots je 10.000 Einwohner vorhanden sind.

Diese Hotspots können über mindestens eine der folgenden Login-Varianten genutzt werden:

1. Ohne Login-Seite, nur per Verbinden mit dem unverschlüsselten WLAN („Freier Hotspot“)
2. Einfach per Mausklick (Auch „freier Hotspot“)
3. Mit WPA2-Schlüssel, der für alle Nutzer am Standort gleich ist
4. Per Voucher, Ticket mit Zugangsdaten für bestimmte Zeit und/oder Datenvolumen
5. Per Registrierung beim Anbieter, zumindest mit E-Mail-Adresse und/oder SMS
6. Für Bestandskunden des jeweiligen Internet-Service-Providers (ISP)

Das Entscheidende für den Nutzer wie auch für den Standort Deutschland im internationalen Vergleich ist, dass der Nutzer Zugriff auf das Internet bekommen kann, wenn er es braucht. Das ist mit all den genannten Zugangsarten mit Ausnahme der Beschränkung auf Bestandskunden des ISPs gegeben.

An den typischen Standorten, an denen Kunden, Gästen, Geschäftsleuten oder Touristen ein Internetzugang angeboten werden soll, achten die Standortinhaber selbstverständlich darauf, dass ihrer jeweiligen Zielgruppe die Nutzung auch möglich ist. Anders sieht es bei den DSL- und Kabel-Routern aus, die in Privathaushalten stehen und parallel zum Internetanschluss des Haushaltes einen WLAN-Hotspot beinhalten. Während diese Art von Hotspots von der Telekom jedem für ein geringes Entgelt und einfacher Online-Zahlung zur Verfügung stehen, sind die mehr als 1 Million WLAN-Hotspots von Vodafone für Dritte nicht zugänglich.[4, 5]
Das liegt aber nicht an der Störerhaftung sondern ist die freie Entscheidung eines Unternehmens darüber, wer seine Infrastruktur zu welchen Konditionen nutzen darf.

Diese Entscheidung wird täglich zigfach im Kleinen von Standortinhabern für Ihren WLAN-Hotspot getroffen und fällt in Deutschland häufig zugunsten von mehr Kontrolle und damit weniger freien Zugängen aus.
Auch dies hat nichts mit der Störerhaftung zu tun.

---

2 „Deutschland liegt mit durchschnittlich 1,87 W-LAN-Hotspots auf 10.000 Einwohner“ auf der Seite http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan.html (Stand 13.12.2015)

3 Siehe http://www.bundesnetzagentur.de/cln_1422/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/WLanUeberwachung/WLanUeberwachung_node.html

4 http://www.hotspot.de/content/tarife_2.html und http://www.hotspot.de/content/tarife_pass.html

5 https://zuhauseplus.vodafone.de/internet-telefon/wlan-hotspots/homespot-service.html und https://zuhauseplus.vodafone.de/internet-telefon/wlan-hotspots/wlan-hotspot-flat.html

Die oben genannten 187 Hotspots pro 10.000 Einwohner entsprechen rund 1,5 Mio. Hotspots in Deutschland. Selbst wenn man von diesen 1 Mio. Hotspots von Vodafone, die nicht für jedermann zugänglich sind, abzieht, so bleibt eine Hotspot-Dichte, die sich im internationalen Vergleich sehen lassen kann.

Angesichts dieser tatsächlichen Zahlen ist fraglich, ob überhaupt ein Problem besteht und somit die Gesetzesänderung überhaupt notwendig ist. Wenn es wirklich noch ein Problem mit der WLAN-Verbreitung in Deutschland geben sollte, so wird dies mittelfristig auch ohne Gesetzesänderung durch den laufenden massiven Ausbau gelöst werden.

Die Bundesnetzagentur hat dies schon erkannt und im Jahr 2015 festgestellt, „dass die **ständig wachsenden Marktanteile** und die nun auch vorliegenden technischen Standards eine Einbeziehung von WLAN-bezogenen Internetdiensten (z. B. Hotspot-Dienst) in die Überwachung rechtfertigen.“ [3]

2.2 These 2: Ursache ist die Störerhaftung

Als Ursache für die angeblich geringe Anzahl von WLAN-Hotspots wird die Störerhaftung angeführt und es wird behauptet, dass vor allem kleinere Unternehmen wie Cafés oder Hotels trotz des damit verbundenen Wettbewerbsnachteils oft auf die Bereitstellung von WLAN-Internetzugängen und damit auf potenzielle Kunden verzichten würden.

Fakt ist: Kein Unternehmer muss heute aus Haftungsgründen auf das Anbieten eines WLAN-Hotspots verzichten!

Das Problem kann ein Café bereits seit 2006 für 9,95 EUR monatlich aus der Welt schaffen, indem es Kunde von HOTSPLOTS wird. Etliche weitere Unternehmen bieten ähnliche Lösungen an.

Wie kommt es dennoch zu der Behauptung, dass viele Unternehmen aufgrund der Störerhaftung auf das Anbieten eines WLAN-Hotspots verzichten würden? Das Ausräumen eines Wettbewerbsnachteils dürfte kaum an 10 EUR im Monat scheitern.

Um dies zu verstehen, lohnt es, den Markt für Hotspot-Lösungen aus Sicht eines kleinen interessierten Unternehmens zu betrachten. Aus Sicht dieses potenziellen WLAN-Betreibers gibt es drei Kategorien von Hotspots:

a) Hotspots die von Providern inklusive Internetanschluss bereitgestellt werden (Telekom, Vodafone/KDG, HOTSPLOTS etc.)
   Die Providerpflichten werden vom Hotspot-Dienstleister erfüllt und dieser ist Ansprechpartner für Ermittlungsbehörden und Abmahnanwälte. In der Praxis spielen Anfragen von Abmahnanwälten jedoch keine Rolle. Anfragen von Ermittlungsbehörden werden professionell von Fachleuten beantwortet.

b) Hotspots mit VPN-Routing. Das hat HOTSPLOTS bereits 2006 eingeführt und es gibt inzwischen mehrere Nachahmer.
   Dabei kann der Standortinhaber seinen eigenen Internetanschluss nutzen, wird aber dennoch nicht für seine Nutzer in Störerhaftung genommen. Die Providerpflichten werden vom Hotspot-Dienstleister erfüllt und dieser ist Ansprechpartner für Ermittlungsbehörden und Abmahnwälte. In der Praxis spielen Anfragen von Abmahnanwälten jedoch keine Rolle. Anfragen von Ermittlungsbehörden können professionell von Fachleuten beantwortet werden.

c) Lokale Hotspot-in-a-box-Lösungen, die von Hardware-Herstellern über Distributoren in den Fachhandel gegeben werden, der es an Hotels etc. verkauft. Das sind – solange es Störerhaftung gibt – aus unserer Sicht meist keine empfehlenswerten Hotspot-Lösungen, weil alle Verantwortung für IT-Sicherheit, Datenschutz, Anpassungen an geänderte Gesetzeslage etc. in die Hände der Kunden (Café-Betreiber, Hoteliers etc.) gelegt wird, die dafür typischerweise keine Fachleute sind. Der Kunde bleibt Ansprechpartner für Behörden und Abmahnanwälte.

Während in der Problembeschreibung des Gesetzesentwurfes die Aussage, dass für den konstatierten Mangel an WLAN-Hotspots die Störerhaftung verantwortlich sei, nicht belegt wird, führt das BMWi auf seiner Seite folgende Statistik an:

> „Vor allem kleinere Unternehmen wie Cafés oder Hotels verzichten deshalb trotz des damit verbundenen Wettbewerbsnachteils oft auf die Bereitstellung von WLAN-Internetzugängen und damit auf potentielle Kunden: Einer Umfrage zufolge schrecken 59 Prozent der befragten geschäftlichen und privaten Nutzer wegen Haftungsrisiken und 43 Prozent wegen Sicherheitsbedenken davor zurück, einen Hotspot anzubieten."

Die Umfrage, auf die sich das BMWi stützt, stammt von einem Hardwarehersteller aus der oben genannten Kategorie c), die dieser im Februar/März 2014 unter seinen eigenen Kunden und Website-Besuchern, Social-Media und den Newsletter-Empfängern eines Hotelsverbandes, durchgeführt hat. Die insgesamt 320 Umfrageteilnehmer waren mehrheitlich Privatpersonen, die Gesamtanzahl der angesprochenen Personen ist nicht angegeben. Der Wortlaut des Fragenkatalogs wurde ebenfalls nicht veröffentlicht. 60 Prozent der Teilnehmer sind in der IT/Telekommunikationsbranche tätig! Das ist keinesfalls repräsentativ für die genannten kleineren Unternehmen wie Cafés oder Hotels. Wieviele der verbleibenden 40 % der Teilnehmer aus der Gastronomie oder Hotellerie kommen und ob überhaupt welche dabei waren, ist nicht angegeben.
Die im Gesetzesentwurf unter Zi. A sowie in der Stellungsnahme des Bundesrates und auf der Website des BMWi aufgestellte Behauptung kann aus dieser Umfrage nicht abgeleitet werden. Ebenso gut könnte man schlussfolgern, dass Cafés und Hotels WLAN-Hotspots haben, aber IT-Unternehmen wegen Bedenken zur Sicherheit und Haftung auf ein solches Angebot verzichten.
Und selbst wenn es zutreffend wäre, dass vor allem kleinere Unternehmen wie Cafés oder Hotels auf ein WLAN-Angebot aufgrund der Störerhaftung verzichten, wäre es so, dass der mögliche Zugewinn an WLAN-Hotspots nur in einem Bereich läge, wie er derzeit ohnehin in wenigen Monaten durch neue Inbetriebnahmen erreicht wird. Denn 43 % der Befragten hatten bereits vor 21 Monaten einen Hotspot angeboten und 43 % der Übrigen hätten damals, selbst ohne Haftungsrisiken, allein aufgrund von Sicherheitsbedenken keinen Hotspot angeboten.
Die meisten der 57 %, die zum Zeitpunkt der Umfrage keinen Hotspot angeboten haben, betreiben aufgrund der Hotspot-Zuwachsraten in Deutschland vermutlich mittlerweile einen und um die Übrigen zu überzeugen, braucht es nicht nur eine Klärung der Bedenken zur Haftung, sondern auch zur Sicherheit. Beides können spezialisierte Hotspot-Dienstleister bieten.

Für die Firmen, die Lösungen aus den Kategorien a und b anbieten, und deren Kunden stellt die Störerhaftung kein Hindernis dar.

2.2.1 Hotspot-Boom durch Ausweitung des Providerprivilegs?

Für die Anzahl der Hotspots, die von professionellen Dienstleistern eingerichtet werden, hat die Störerhaftung folglich keine negativen Auswirkungen. Bezüglich der Anzahl von Hotspots, die selbst bei genereller Abschaffung der Störerhaftung von privaten und gewerblichen Anbietern selbstständig, also ohne Hotspot-Dienstleister, aufgestellt werden würden, lässt sich nur mutmaßen. Es gibt aber einige Indizien dafür, dass sich an der bestehenden Situation nichts Gravierendes ändern würde, denn private Anbieter könnten schon längst Hotspots frei oder gegen Bezahlung anbieten, tun es jedoch in der Mehrheit nicht:

1. Vodafone-Kunden mit einem Flatrate-Tarif können de facto nicht für Urheberrechtsverletzungen in Anspruch genommen werden. Dennoch gibt es keine Anzeichen, dass diese vermehrt freie WLAN-Hotspots einrichten würden. Dass Vodafone die dynamischen IP-Adressen seiner Kunden gar nicht über das Verbindungsende hinaus speichert und somit eine Verfolgung von Urheberrechtsverletzungen durch die

Rechteinhaber gar nicht möglich ist, war bisher vielleicht Insiderwissen, ist aber inzwischen in der Stellungnahme der WALDORF FROMMER Rechtsanwälte auf der Website des BMWi veröffentlicht.[6] Darin wird sogar gezeigt, dass Vodafone-Kunden im Mittel viel mehr Urheberrechtsverletzungen begehen als Kunden anderer Provider, insbesondere die der Telekom. Die Nutzer, die das wissentlich ausnutzen, könnten ebenso einen öffentlichen Hotspot anbieten. Das tun sie aber nicht und wir sehen keinen Grund anzunehmen, dass das nach einem Wegfall der Störerhaftung anders wäre.

2. Freifunk ist trotz Störerhaftung sehr aktiv, das Providerprivileg ist gerichtlich bestätigt worden, und dennoch ist die Hotspot-Ausbreitung sehr überschaubar.

3. Auch Unternehmen haben versucht, Produkte im Bereich des privaten „DSL-Teilens“ anzubieten. Der Pionier sofa networks GmbH spielt keine Rolle mehr, Fon hat vor der Partnerschaft mit der Telekom viele Router verteilt, darüber aber nur wenige Hotspots realisieren können und auch HOTSPLOTS ist mit einem solchen Produkt vor elf Jahren gestartet, hat damit aber nie nennenswerte Standortzahlen erreicht.

Die Ursache dafür, dass nicht die Mehrheit privater WLANs zu freien Hotspots werden, liegt folglich nicht in der Störerhaftung sondern in der Mentalität. Die Bürger können selbst entscheiden und die meisten sagen: „Das will ich nicht.“

Unter Zi. 2.1 wurde zudem bereits erläutert, dass viele gewerbliche Hotspotbetreiber ebenfalls von der Möglichkeit ihre WLAN-Zugänge zu öffnen absehen. Im öffentlichen Bereich verhält es sich nicht anders: Die Berliner Senatsverwaltung bemüht sich seit Jahren, öffentliches WLAN in die Stadt zu bekommen. HOTSPLOTS hat seit Jahren praktisch alle Bibliotheken mit WLAN-Hotspots ausgestattet. Diese könnten natürlich auch in die Fläche strahlen, aber daran haben die Bibliotheksverwaltungen typischerweise kein Interesse, sondern wollen den Zugang nur für die Besucher ihrer Häuser ermöglichen. Der Standortinhaber entscheidet und das ist auch gut so.

3 Zum Entwurf des § 8 TMG

3.1 Zu § 8 Abs. 3 TMG

Die hier erfolgte Klarstellung ist gut, hat aber in der Praxis keinerlei Auswirkungen.

HOTSPLOTS hat diese Auffassung schon immer vertreten, in der juristischen Literatur hat sie sich durchgesetzt, die deutschen Gerichte vertreten zumindest seit 2014 diese Auffassung und das LG München hat unter anderem diesen Punkt dem EuGH vorgelegt.[7]

Zu fragen ist jedoch: Welche Pflichten hat der Diensteanbieter zu erfüllen? Belehrung und Sicherungsmaßnahmen nach TMG und Meldepflicht, Sicherheitskonzept, Vorratsdatenspeicherung und Telekommunikationsüberwachung nach TKG?

3.2 Zu § 8 Abs. 4 TMG

Die Wahl der unbestimmten Rechtsbegriffe „zumutbare Maßnahmen“ und „angemessene Sicherungsmaßnahmen“ ist bedauerlich, weil damit entgegen der angestrebten rechtlichen Klarstellung künftig wohl doch Gerichte in Bezug auf konkrete Maßnahmen zu klären haben, was zumutbar und was angemessen ist.

---

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

7 Siehe auch http://www.offenenetze.de/2015/03/03/der-wlan-gesetzesentwurf-der-bundesregierung-%C2%A7-8-tmg-im-detail-ein-zweiter-blick-oder-doch-lieber-weggucken/ Zi. 3 b

Die beispielhaft genannten Maßnahmen

1. angemessene Sicherungsmaßnahmen gegen den unberechtigten Zugriff auf das drahtlose lokale Netzwerk ...
2. Zugang zum Internet nur dem Nutzer gewährt, der erklärt hat, im Rahmen der Nutzung keine Rechtsverletzungen zu begehen

beschreiben genau das, was derzeit bei professionellen Hotspot-Dienstleistern üblich ist.

Wer bei den angemessenen Sicherungsmaßnahmen jedoch an WPA2-Verschlüsselung denkt, der übersieht, dass mit dem „unberechtigten Zugriff“ nicht das bloße Verbinden mit dem WLAN gemeint sein kann. Denn ohne Verbindung zum WLAN wäre auch der Zugriff auf das Internet, um den es bei einem freien öffentlichen WLAN-Hotspot ja gerade geht, nicht für jedermann möglich. Es kann daher kein unberechtigtes Verbinden mit dem WLAN geben. Im Entwurf heisst es korrekt „Zugriff auf das lokale Netzwerk“, also auf die Infrastruktur bestehend aus Access Points und Hotspot-Router. Dass diese vor unberechtigtem Zugriff durch Hotspot-Nutzer geschützt werden muss, ist für einen professionellen Hotspot-Dienstleister selbstverständlich und darüber hinaus im Sicherheitskonzept nach § 109 TKG zu dokumentieren.

Außerdem wäre der Sicherheitsgewinn durch eine Verschlüsselung des WLANs nicht relevant, denn das Internet ist ein unsicheres Medium und nicht nur die wenigen Meter WLAN am Hotspot. Kritische Daten, wie etwa Online-Banking, müssen immer Ende-zu-Ende verschlüsselt sein, also vom Endgerät bis zum Server. Damit ist auch das WLAN abgesichert. Das wesentliche Angriffsszenario einer Man-in-the-middle-Attacke, bei dem sich ein Angreifer als Access Point des Hotspots ausgibt und die Daten über seine technische Infrastruktur leitet, ist mit einer WPA2-Verschlüsselung, bei der alle den gleichen bekannten Schlüssel nutzen, ganz genauso möglich, wie ohne Verschlüsselung. Eine Verschlüsselung könnte dabei sogar das Risiko erhöhen, wenn sich die Nutzer in vermeintlicher Sicherheit wähnen.
Der Mehrgewinn an Sicherheit beschränkte sich darauf, dass es für einen Angreifer etwas aufwändiger wäre, zu sehen, welche Webseiten man besucht.
Im Gegenzug stünde eine geringere Nutzerfreundlichkeit, was dem erklärten Ziel, die Dichte einfach zu nutzender Hotspots zu erhöhen, entgegen stünde.

Für die Standortinhaber, die keinerlei Kontrolle über die Nutzung Ihres WLAN-Hotspots wünschen und deren Erstnutzer so schnell und so einfach wie möglich ins Internet kommen sollen, ist das Einloggen über die Bestätigung der Nutzungsbedingungen Standard. Der Anteil dieser Art von Hotspots ist z. B. bei HOTSPLOTS von Dezember 2014 bis November 2015 von 18 % auf 29 % gestiegen. Die Zahl dieser freien Hotspots steigt sowohl durch Inbetriebnahme neuer Hotspots als auch durch Umstellung bereits bestehender Hotspots stetig an. Das gilt auch für andere Anbieter: So genügt an den Telekom-Hotspots bei McDonalds, die bei der Erhebung des eco-Verbandes ausdrücklich nicht zu den freien Hotspots gezählt wurden, weil vor einem Jahr für Nicht-Telekom-Kunden noch eine Authentifizierung per SMS notwendig war, inzwischen ein einfacher Klick auf einen Button.

Wünschenswert wäre eine Präzisierung, wie der Nutzer seine Erklärung abgeben muss. Diesbezüglich befindet sich der Markt gerade in einer Abwärtsspirale, was den Grad der psychologischen Hürde angeht. Nachdem anonyme Logins an WLAN-Hotspots mit dem Urteil des LG München 2012 offiziell möglich wurden, hatte HOTSPLOTS vom Nutzer vor dem Login das aktive Setzen eines Häkchens gefordert und einen Ausschnitt der Nutzungsbedingungen in einem scrollbaren Textfenster gezeigt. Nachdem praktisch alle Wettbewerber sich mit dem Anzeigen eines Links zu ihren Nutzungsbedingungen begnügt haben, haben auch wir auf Kundenwunsch auf die dominantere Anzeige der Nutzungsbedingungen verzichtet. Bei den Hotspots der Fast-Food-Kette ist nicht einmal mehr das Setzen eines Häkchens notwendig. Da ist es sicher nur eine Frage der Zeit, bis andere Wettbewerber und HOTSPLOTS

diesbezüglich nachziehen werden.
Wenn der Gesetzgeber wünscht, dass die Nutzer zur Kenntnis nehmen, was sie da erklären, könnte er etwas mit einer Anpassung des § 8 TMG bewirken. Der vorgelegte Entwurf bewirkt dies jedoch nicht.

4 § 8 TMG im Kontext von Providerpflichten und Strafverfolgung

Der massive Ausbau von WLAN-Hotspots wird im Moment im Wesentlichen von professionellen Dienstleistern getragen.

Der Effekt sowohl des Gesetzesentwurfes der Bundesregierung als auch der vom Bundesrat geforderten Formulierung des § 8 TMG wäre vermutlich, dass mehr Standortinhaber auf die Leistung professioneller Hotspot-Dienstleister verzichten würden.

Die im Entwurf der Bundesregierung genannten Maßnahmen könnten allein durch einen geeigneten lokalen Router erfüllt werden. Das kann ein preiswerter WLAN-Router mit Open Source Software, wie sie auch Freifunk einsetzt, sein und für die Hersteller der gängigen DSL-Router (Fritz!Box, Speedport etc.) wäre es eine Kleinigkeit, diese Funktionen mit einem Firmware-Update hinzuzufügen.
Mit der vom Bundesrat geforderten Fassung könnte sogar jeder heute genutzte Internet-Router genutzt werden.

Dass davon jedoch keine nachteiligen Effekte auf die Strafverfolgung zu erwarten seien, wie in Anlage 2 Zi. 3 behauptet wird, ist zu bezweifeln.

Dies wird dort erstens damit begründet, dass die Auflagen, etwa zur Umsetzung von Überwachungsmaßnahmen und Erteilung von Auskünften nach § 110 TKG und § 113 TKG, weiterhin für Betreiber oberhalb der Marginaliengrenze gelten. Wenn aber die Mehrheit der Hotspots unter die Marginaliengrenze fällt, so handelt es sich dabei dennoch um die Mehrheit, auch wenn jeder einzelne unterhalb der Marginaliengrenze liegt.

Zweitens wird als Begründung angeführt, dass auch private Anbieter für die Internetanbindung ihrer WLAN-Zugangspunkte die Angebote kommerzieller Accessprovider, die den Rahmenbedingungen des TKG unterliegen, nutzen. Das ist richtig, aber diese Accessprovider sind die Netzbetreiber, die den Internetanschluss stellen. Diese sehen nur den Datenverkehr des Internetanschlusses als Ganzes. Nutzerspezifische Information geht dabei verloren. Aus unserer Erfahrung mit Ermittlungsanfragen können wir sagen, dass die MAC-Adressen für Ermittlungsbehörden von großer Bedeutung sind. Diese werden von HOTSPLOTS derzeit drei Tage lang gespeichert. Erst vor Kurzem hat das BKA Standortangaben und MAC-Adressen im Rahmen von Ermittlungen zu Terrorismusabwehr dankbar entgegen genommen. Auch den umgekehrten Fall, dass Ermittler die MAC-Adressen bereits kannten und uns nach weiteren Informationen fragten, als sich die Verdächtigen an einem unserer Hotspot-Standorte aufhielten, gab es schon. Im konkreten Fall konnten wir aufgrund der bestehenden Datenschutzvorschriften nicht weiterhelfen. Mit der kommenden Telekommunikationsüberwachung könnte es für die Ermittler in solchen Fällen besser aussehen.

Ferner wird in Anlage 2 behauptet, dass eine Zunahme von Urheberrechtsverletzungen nicht zu erwarten sei, weil die Bandbreite von öffentlichen Hotspots dafür typischerweise zu gering sei. Es ist richtig, dass die Freifunk-Software erlaubt, die den Hotspot-Nutzern bereitgestellte Bandbreite zu limitieren. Das erlaubt auch die Software von HOTSPLOTS. Davon wird aber im Regelfall, in dem der Anbieter möchte, dass die Nutzer ein positives Nutzungserlebnis haben, kein Gebrauch gemacht. Richtig ist, dass die Bandbreiten von WLAN-Hotspots immer weiter steigen und dafür typischerweise Anschlüsse mit den höchsten Bandbreiten, die bezahlbar und verfügbar sind, gebucht werden. Bei HOTSPLOTS hat sich das durchschnittliche Datenvolumen pro Hotspot in den letzten 24 Monaten knapp verdoppelt.

Weiter wird angeführt, dass beim Streaming die WLAN-Zugangspunkte gänzlich ungeeignet für die Anbindung der Server, auf denen das gestreamte Material vorgehalten wird, sei. Das ist sicher richtig, die Server stehen in Rechenzentren außerhalb der EU – weshalb nebenbei bemerkt der Entwurf für § 10 TMG diesbezüglich wirkungslos ist. Für Clients, also die Nutzung dieser Streamingdienste, wird aber, sofern technisch möglich, eine ausreichende Bandbreite geboten. Ansonsten hätte der Nutzer auch Probleme mit Videotelefonie und der Nutzung legaler Streamingdienste.

Diese Begründungen sind somit zwar nicht stichhaltig, die Aussage, dass eine Zunahme von Urheberrechtsverletzungen nicht zu erwarten sei, ist dennoch zutreffend. Die tatsächlichen Gründe sind erstens, dass der Gesetzesentwurf weder in der Fassung der Bundesregierung noch mit den Formulierungen des Bundesrates einen wesentlichen Einfluss auf die Anzahl der WLAN-Hotspots in Deutschland haben wird, und zweitens, dass eine Ahndung von Urheberrechtsverletzungen beim jetzigen Stand der Technik und den aktuellen Datenschutzvorschriften des Telekommunikationsgesetzes auch an professionell betriebenen Hotspots de facto nicht stattfindet.

5 Zusammenfassung

Der Entwurf zur Änderung des § 8 TMG ist abzulehnen.

Es besteht keine Notwendigkeit, weil die Versorgung mit WLAN-Hotspots in Deutschland bereits gut ist und der weitere Ausbau zügig voran geht.

Der wesentliche Effekt wäre, dass viele Anbieter auf professionelle Dienstleister verzichten würden, dann unter die Marginaliengrenze fallen würden und somit diese Hotspots von §110 und §113 ausgenommen wären.

Für die Strafverfolgung hätte der Gesetzesentwurf damit negative Auswirkungen.

Berlin, 14.12.2015

Dr. Ulrich Meier

Geschäftsführer