

## STELLUNGNAHME

---

**An:** Ausschuss für Wirtschaft, Verkehr und Landesentwicklung des Hessischen Landtags  
**Kontakt:** Dr. Thomas Sassenberg  
M: +49 152 31083281  
E: [thomas@sassenberg.info](mailto:thomas@sassenberg.info)

**Von:** Dr. jur. Reto Mantz, Dipl.-Inf., Richter am Landgericht Frankfurt am Main  
Dr. Reto Mantz  
M: [rm@wlan-recht.de](mailto:rm@wlan-recht.de)

Dr. Thomas Sassenberg, LL.M.  
Rechtsanwalt  
Fachanwalt für Medien- und Urheberrecht

**Datum:** 02. November 2015

---

### FREIE WLAN-HOTSPOTS IN HESSEN

<b>A. Einführende Zusammenfassung</b> .....	<b>3</b>
<b>B. Beantwortung der Fragen des hessischen Landtags</b> .....	<b>5</b>
I. Rechtliche Rahmenbedingungen .....	5
1. Was ist der rechtliche Unterschied zwischen Content-, Host- und Access-Providern und inwiefern ist diese Einordnung für WLAN-Betreiber von Bedeutung?.....	5
2. Wann erfahren Access-Provider eine Haftungsprivilegierung? .....	5
3. Welche Maßnahmen müssen Access-Provider ergreifen, wenn wiederholte Rechtsverletzungen auftreten? .....	6
4. Welche Haftungsrisiken bestehen derzeit für WLAN-Betreiber, welche der TMG-Privilegierung nicht unterliegen? .....	6
5. Welche Haftungsprivilegierungen sind de lege ferenda denkbar? .....	8
6. Existieren Gründe, zukünftig zwischen privaten und gewerblichen/institutionellen Betreibern zu unterscheiden? .....	10
7. Bestehen neben den zivilrechtlichen Haftungsfragen sicherheitspolitische bzw. strafverfolgungserhebliche Bedenken? .....	11
8. Wie ist die strafrechtliche Verantwortlichkeit von Betreibern offener WLAN-Netze einzuordnen im Hinblick auf Beihilfe, Mittäterschaft und (Eventual-)Vorsatz? .....	12
II. Datenschutz und Datensicherheit .....	13
1. Aus welchen Gründen ist es sinnvoll/nicht sinnvoll Haftungsprivilegierungen nur für verschlüsselte Verbindungen vorzusehen?.....	13

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

2. Bedarf es technischer Auflagen für den Betrieb zur Gewährung von Datenschutz- und Datensicherheit? Gibt es allgemeine Standards? .....	13
III. Internationaler Vergleich .....	16
1. In welchem rechtlichen Rahmen im Hinblick auf zivil- und strafrechtliche Aspekte operieren WLAN-Betreiber im internationalen Vergleich?.....	16
2. Welche Erkenntnisse lassen sich hieraus für Deutschland und Hessen ableiten? ....	16
IV. Ausbau.....	17
1. Welche Gründe sprechen für und gegen öffentliche Förderung bei Aufbau und/oder Betrieb von WLAN-Netzen? .....	17
2. Welche Instrumente der Förderung existieren? Welche sind Ihnen bekannt? Welche Formen der Förderung wären denkbar? .....	17
3. Welche Betreibermodelle existieren? Welche Modelle werden am häufigsten gewählt und wie kann man dies erklären?.....	18
4. Welche Rolle kann das Modell „freifunk“ für den Ausbau des WLAN in Hessen spielen?.....	18
5. Welche Gründe sprechen für eine Zusammenarbeit der Kommunen, der Städte, der Landkreise und des ÖPNV beim Aufbau eines öffentlichen WLANs? Welche Gründe sprechen dagegen?.....	19
6. Wer trägt die Kosten für den Aufbau und den Betrieb von WLAN-Netzen? .....	20
V. Wirtschaftliche Bedeutung und Effekte .....	20
1. Welchen Nutzen haben Städte und Gemeinden durch freie öffentlich zugängliche WLAN-Netze? .....	20
2. Haben freie öffentlich zugängliche WLAN-Netze auch für die Tourismuswirtschaft eine Bedeutung? .....	21
3. Welchen Nutzen haben andere Wirtschaftssektoren und Branchen durch frei öffentlich zugängliche WLAN-Netze?.....	22
4. Sind Auswirkungen auf (lokale) Telekommunikationsbetreiber zu erwarten, die inzwischen Vergleichbare Leistungen (z.B. LTE) im Rahmen von Nutzerverträgen gegen Rechnung zur Verfügung stellen? .....	23
5. Was ist beim Aufbau eines öffentlich geförderten und/oder betriebenen WLAN-Netzes im Hinblick auf das Wirtschaftsverwaltungsrecht zu beachten, wenn bestehende WLAN-Angebote (z.B. durch die Telekom) bestehen? .....	24
VI. Förderprojekte im Bundesvergleich .....	25
1. Welche staatlich geförderten WLAN-Projekte existieren derzeit in Deutschland? .....	25

# Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

## A. EINFÜHRENDE ZUSAMMENFASSUNG

### I. Derzeitige Rechtslage

- (1) Der im internationalen Vergleich geringe Ausbau von öffentlichen WLAN-Hotspots lässt sich damit erklären, dass eine große Unsicherheit potentieller Hotspot-Betreiber hinsichtlich einer möglichen Inanspruchnahme aufgrund von Nutzern des Hotspots über das Internet begangener Rechtsverletzungen besteht. Teilweise wird zudem angeführt, dass kleinere Anbieter mit der Umsetzung der telekommunikationsrechtlichen Anforderungen überfordert sind.
- (2) Es besteht Einigkeit dahingehend, dass der Betreiber eines öffentlichen WLAN-Hotspots als sog. Access-Provider der **telemedienrechtlichen Haftungsprivilegierung** unterfällt und – vereinfacht – im Rahmen seines typischen Verhaltens als Provider nicht in Anspruch genommen werden kann. Nach der bisherigen Rechtsprechung des Bundesgerichtshof (BGH) gilt diese Privilegierung jedoch nicht für Ansprüche, welche darauf gerichtet sind, dass ein bestimmtes rechtswidriges Verhalten zukünftig zu unterbinden ist (sog. Unterlassungsansprüche). Für diese Unterlassungsansprüche gilt im Grundsatz, dass der Betreiber eines WLAN-Hotspots verpflichtet ist, die ihm zumutbaren Maßnahmen zu ergreifen, um zukünftige Rechtsverletzungen zu verhindern, ohne dass ihm hierbei sein Geschäftsmodell unmöglich gemacht wird. Kommt er den ihm zumutbaren Maßnahmen nach, kann er nicht als sog. **Störer** in Anspruch genommen werden. Welche Maßnahmen dies sind, wurde in der höchstrichterlichen Rechtsprechung bisher noch nicht konkretisiert. Die Instanzgerichte gehen bislang zutreffend davon aus, dass keine Maßnahmen zu ergreifen sind.
- (3) Als **Maßnahmen** werden in diesem Zusammenhang insb. die Verschlüsselung und die Nutzeridentifikation sowie das Sperren und Filtern diskutiert. Die insoweit diskutierten Optionen tragen jedoch nicht zur Rechtssicherheit bei, laufen dem Interesse der Möglichkeit einer einfachen Nutzung entgegen und stellen zudem das Geschäftsmodell des offenen und entgeltfreien WLANs in Frage. Dies hat zur Folge, dass der Betreiber eines offenen WLAN-Hotspots auch dann nicht in Anspruch genommen werden kann, wenn er keine der genannten Maßnahmen ergriffen hat.

### II. Aktuelle Entwicklungen

- (4) Derzeit sind Verfahren vor dem Europäischen Gerichtshof (EuGH) und dem BGH anhängig, welche zu einer Klärung der offenen Rechtsfragen führen könnten. Der BGH befasst sich in zwei Verfahren mit der Frage, welche Maßnahmen einem Access-Provider zugemutet werden können. Das Landgericht München I hat dem EuGH die Frage vorgelegt, ob die Haftungsprivilegierung des § 8 TMG auch für Unterlassungsansprüche zur Anwendung kommt – dann würde sich die Frage einer möglichen Inanspruchnahme als Störer erst gar nicht stellen – und welche Maßnahmen andernfalls dem Provider zugemutet werden können.

## **Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“**

- (5) Gleichzeitig hat die Bundesregierung einen Gesetzesentwurf verabschiedet, der eine Änderung des Telemediengesetzes (TMG) vorsieht, und der die Frage der Haftungsprivilegierung für WLANs klären soll. Zu Recht ist dieser Gesetzesentwurf auf Kritik gestoßen. Es ist nicht damit zu rechnen, dass er das Ziel der Förderung des Aufbaus von öffentlichen WLANs erreichen wird, da er insbesondere das (zulässige) Geschäftsmodell öffentlich zugänglicher WLANs in Frage stellt.
- (6) Am 16.10.2015 hat der Bundestag zudem das *„Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“* verabschiedet (BT-Drs. 18/6391). Die Verpflichtung zur sog. Vorratsdatenspeicherung ist von allen Erbringern von öffentlichen Telekommunikationsdienstleistungen umzusetzen. Auch dieser führt zu einer Unsicherheit bei bestehenden und potentiellen Betreibern von öffentlich zugänglichen WLAN-Hotspots.

### **III. Förderung durch die öffentliche Hand**

- (7) Der Vergleich mit anderen Ländern zeigt, dass eine öffentliche Förderung des Ausbaus von öffentlichen WLANs geboten ist und u.a. der Wirtschaft zugute kommen würde. Es ist nicht davon auszugehen, dass dies Mobilfunk- oder Festnetznetzanbieter beeinträchtigen würde. Eine Förderung muss dabei nicht per se finanzieller Art sein. In der Regel verfügen Städte, Kreise und Länder aufgrund ihrer innerstädtischen Gebäude über eine Infrastruktur, welche Anbietern den Aufbau eines öffentlichen WLANs erheblich erleichtert.

# Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

## B. BEANTWORTUNG DER FRAGEN DES HESSISCHEN LANDTAGS

### I. RECHTLICHE RAHMENBEDINGUNGEN

#### 1. WAS IST DER RECHTLICHE UNTERSCHIED ZWISCHEN CONTENT-, HOST- UND ACCESS-PROVIDERN UND INWIEFERN IST DIESE EINORDNUNG FÜR WLAN-BETREIBER VON BEDEUTUNG?

(8) Das TMG und die E-Commerce-Richtlinie, deren Umsetzung das TMG dient, unterscheiden allgemein zwischen verschiedenen Diensteanbietern. Die Unterscheidung zwischen den verschiedenen Anbietern ist für alle Diensteanbieter von Bedeutung, da an diese Einordnung jeweils unterschiedliche Folgen geknüpft werden. Diensteanbieter sind u.a. der Content Provider (§ 7 Abs. 1 TMG), der Access Provider (§ 8 TMG) und der Host Provider (§ 10 TMG):

- **Content Provider** ist jeder Diensteanbieter der selbst (eigene) Inhalte bereitstellt, beispielsweise der Betreiber einer redaktionell betreuten Zeitungswebseite oder der Inhaber eines privaten Blogs, auf dem über den letzten Urlaub berichtet wird. Content Provider sind gemäß § 7 Abs. 1 TMG für ihre Inhalte nach den allgemeinen Gesetzen verantwortlich. Für sie greift keine Haftungsprivilegierung.
- **Access Provider** ist nach § 8 Abs. 1 TMG ein Diensteanbieter, der fremde Informationen in einem Kommunikationsnetz übermittelt oder den Zugang zur Nutzung von fremden Informationen vermittelt. Nach der Definition gehört hierzu insbesondere jeder, der den Zugang ins Internet vermittelt.
- **Host Provider** ist gemäß § 10 TMG, wer fremde Informationen für Nutzer speichert. Hierzu gehören insbesondere Plattformbetreiber, die ihren Nutzern die Möglichkeit geben, Informationen zum Abruf im Internet bereitzustellen, beispielsweise eBay, Blog-Portale, E-Mail-Dienste und sogenannte Filehoster.

#### 2. WANN ERFAHREN ACCESS-PROVIDER EINE HAFTUNGSPRIVILEGIERUNG?

- (9) Nach § 8 TMG ist eine Verantwortlichkeit des Access Providers ausgeschlossen, wenn es sich bei der von ihm übermittelten Information um (i.) eine fremde Information handelt, der Access Provider (ii.) die Übermittlung nicht veranlasst, (iii.) den Adressaten nicht ausgewählt, (iv.) die übermittelten Informationen nicht ausgewählt oder verändert und (v.) nicht mit dem rechtsverletzenden Nutzer absichtlich zusammengearbeitet hat. Zusammenfassen lässt sich dies dahingehend, dass Access Provider im Hinblick auf die von ihnen über das Netzwerk übermittelten Informationen eine streng neutrale Stellung einnehmen müssen. Weitere Anforderungen sieht § 8 TMG – nach derzeitigem Stand – nicht vor.
- (10) Zur Bedeutung der Haftungsprivilegierung für WLAN-Betreiber und insb. zur Anwendbarkeit auf Unterlassungsansprüche siehe auch die Antwort zu Frage I.4 (Rn. 14).

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

### 3. WELCHE MAßNAHMEN MÜSSEN ACCESS-PROVIDER ERGREIFEN, WENN WIEDERHOLTE RECHTSVERLETZUNGEN AUFTRETEN?

- (11) Es ist noch nicht abschließend geklärt, welche Maßnahmen Access Provider ergreifen müssen, nachdem eine Rechtsverletzung auftritt. In diesem Zusammenhang werden verschiedene Maßnahmen diskutiert. Einerseits geht es dabei im weiteren Sinne um „*Sperren und Filtern*“, namentlich durch DNS-Sperren, IP-Sperren, URL-Sperren und Verkehrsfilter. Im Falle wiederholter Rechtsverletzungen eines Nutzers wurde vor einigen Jahren die Aussprache von Verwarnungen verlangt – meist unter den Bezeichnungen „*Three-Strikes-Modell*“ oder „*abgestufte Erwiderung*“. Umsetzungen in anderen Ländern haben sich jedoch als unpraktikabel und unverhältnismäßig erwiesen (näher *Sassenberg/Mantz, WLAN und Recht, 2014, Rn. 236 m.w.N.*). Im Hinblick auf WLANs werden derzeit teilweise Verschlüsselung, Registrierung und Belehrung der Nutzer diskutiert (vgl. BT-Drs. 18/5088).
- (12) In der Rechtsprechung sind Pflichten für Access Provider auch bei mehrfachem Auftreten von Rechtsverletzungen bisher als gesetzeswidrig oder unverhältnismäßig abgelehnt worden. So haben das OLG Hamburg und das OLG Köln DNS-Sperren, IP-Sperren, URL-Sperren und Verkehrsfilter als unzumutbare Maßnahmen angesehen (OLG Köln GRUR 2014, 1081 – Goldesel; OLG Hamburg GRUR-RR 2014, 140 – 3dl.am; die Entscheidungen sind derzeit als Revision beim BGH anhängig, Entscheidungen werden für den 26.11.2015 erwartet), wobei nach Auffassung von OLG Köln und OLG Hamburg insbesondere URL-Sperren und Verkehrsfilter Eingriffe in das Fernmeldegeheimnis darstellen. Verschlüsselung, Registrierung und Belehrung sind von Access Providern bisher nicht verlangt worden.
- (13) Es hat sich herausgestellt, dass diese Maßnahmen praktisch unwirksam und leicht zu umgehen sind. Gegen DNS-Sperren wird insbesondere angeführt, dass sie zum einen durch Verwendung alternativer DNS-Server leicht zu umgehen sind (OLG Hamburg, MMR 2009, 631 – Usenet), und dass sie dazu führen, dass nicht nur rechtswidrige Inhalte blockiert werden, sondern auch andere, legale Inhalte, was als „*Overblocking*“ bezeichnet wird (OLG Hamburg MMR 2009, 631 – Usenet; OLG Hamburg GRUR-RR 2014, 140 (147) – 3dl.am; OLG Köln GRUR 2014, 1081 – Goldesel). Gleiches gilt für URL-Sperren. Filter, die auf den Datenverkehr selbst abstellen, sind vor allem problematisch, weil die Inhalte zur Kenntnis genommen werden, was einen Verstoß gegen das Fernmeldegeheimnis bedeutet. Darüber hinaus können auch solche Filter Rechtsverletzungen nicht sicher erkennen und zum Overblocking führen.

### 4. WELCHE HAFTUNGSRSIKEN BESTEHEN DERZEIT FÜR WLAN-BETREIBER, WELCHE DER TMG-PRIVILEGIERUNG NICHT UNTERLIEGEN?

- (14) Nach §§ 7 ff. TMG und in Umsetzung von Art. 12 bis 15 E-Commerce-Richtlinie sollen Internet Service Provider für Rechtsverletzungen ihrer Nutzer nicht haften. Insbesondere sollen ihnen keine proaktiven Überwachungspflichten obliegen. Daher schließen diese – unter den jeweiligen Voraussetzungen – eine Verantwortlichkeit der Internet Service Provider für die rechtswidrigen Handlungen ihrer Nutzer aus. Für

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

Access Provider greift hierbei die Privilegierung in § 8 TMG, nach dem eine Verantwortlichkeit unter den oben genannten Voraussetzungen ausgeschlossen ist.

- (15) Es besteht derzeit kein ernsthafter Zweifel daran, dass auch der Betreiber eines WLANs die Voraussetzungen des § 8 TMG erfüllt (LG München I GRURInt 2014, 1166 – Bring mich nach Hause; AG Berlin-Charlottenburg CR 2015, 192; AG Hamburg CR 2014, 536; AG Hamburg, Urt. v. 24.6.2014 – 25b C 924/13; *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 211; *Röhrborn/Katko*, CR 2002, 882; *Hoffmann*, in: *Spindler/Schuster*, Recht der elektronischen Medien, 3. Aufl. 2015, § 8 TMG Rn. 17; *Spindler*, CR 2010, 592 (595); *Altenhain*, in: MünchKommStGB, 2. Aufl. 2010, vor § 7 TMG, Rn. 43; *Kaeding*, CR 2010, 164 (168); *Mantz*, Rechtsfragen offener Netze, 2008, 48).
- (16) Danach besteht kein Risiko des Betreibers eines WLANs, für Rechtsverletzungen seiner Nutzer strafrechtlich in Anspruch genommen zu werden oder Schadensersatz leisten zu müssen.
- (17) Die Privilegierung findet nach ständiger Rechtsprechung des BGH aber keine Anwendung auf Unterlassungsansprüche, also auf Ansprüche aus Störerhaftung (BGH GRUR 2004, 693 (694) – Schöner Wetten; BGH GRUR 2004, 860 (862 f.) – Internetversteigerung I; auf die Haftung aufgrund Verkehrspflichten soll hier nicht näher eingegangen werden, für sie gilt im Ergebnis dasselbe wie für die Störerhaftung, vgl. *Mantz/Sassenberg*, NJW 2014, 3537 (3541)). Dies ist zwar in der juristischen Literatur mit Blick auf eine Vereinbarkeit Art. 15 E-Commerce-Richtlinie wiederholt kritisiert worden, der EuGH hat jedoch im Rahmen der Entscheidung UPC Telekabel trotz Art. 12 bis 15 E-Commerce-Richtlinie Prüfpflichten nicht rundheraus abgelehnt (EuGH GRUR 2014, 468 – UPC Telekabel/Constantin Film). Auf der anderen Seite greift der BGH die Privilegierung mittlerweile auch bei der Störerhaftung ausdrücklich auf und integriert die Vorgaben der E-Commerce-Richtlinie, des TMG und der Rechtsprechung des EuGH in die Bewertung der Prüfungs- und Überwachungspflichten im Rahmen der Störerhaftung (OLG Hamburg GRUR-RR 2014, 140 – 3dl.am; KG Berlin MMR 2014, 46; *Volkmann*, K&R 2013, 257 (258)). Die Frage der Zulässigkeit der Einschränkung der Privilegierung liegt mittlerweile als Vorlagefrage dem EuGH vor. Das LG München I hat Ende 2014 einen Fall eines WLAN-Betreibers zum Anlass genommen, diese und andere Fragen zu § 8 TMG dem EuGH vorzulegen (LG München I GRUR Int. 2014, 1166 – Bring mich nach Haus).
- (18) Als Haftungsrisiko verbleibt beim Betreiber eines WLANs daher die Haftung auf Unterlassung nach den Grundsätzen der sog. Störerhaftung. Dies bedeutet, dass der Betreiber verpflichtet sein kann, bestimmte Maßnahmen zur Verhinderung von Rechtsverletzungen zu ergreifen. Als Störer kann dabei grundsätzlich derjenige in Anspruch genommen werden, der (i.) adäquat-kausal an einer Rechtsverletzung mitwirkt und (ii.) hierbei seine so genannten Prüfungs- und Überwachungspflichten verletzt hat. Ein Verschulden ist hierfür nicht erforderlich. Die erste Voraussetzung der Störerhaftung, eine adäquat-kausale Mitwirkung an der Rechtsverletzung des Nutzers, liegt jedenfalls in der Vermittlung des Zugangs zum Internet – auch über WLAN – vor

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

(BGH NJW 2010, 2062 – Sommer unseres Lebens; LG Frankfurt a.M., MMR 2011, 401; LG Frankfurt a.M. GRUR-RR 2013, 507 – Ferienwohnung; a.A. noch OLG Frankfurt a.M., MMR 2008, 603.) Insofern stellt sich die Frage, ob und gegebenenfalls wann durch den WLAN-Betreiber Prüfungs- und Überwachungspflichten verletzt werden. Hierunter werden bestimmte – nicht genau konkretisierte – Maßnahmen verstanden, die ein Betreiber zur Verhinderung von Rechtsverletzungen ergreifen soll. Die konkreten Pflichten sind (bisher) nicht gesetzlich geregelt, sondern werden maßgeblich von der Rechtsprechung in Einzelfallentscheidungen herausgebildet. Ein anschauliches Beispiel für eine auf Grund von Prüfungs- und Überwachungspflichten zu ergreifende Maßnahme kann die Pflicht von Eltern sein, ihre minderjährigen Kinder vor der Erlaubnis der Nutzung des familiären Internetzugangs darauf hinzuweisen, dass der Internetanschluss nicht für rechtswidrige Handlungen genutzt werden soll (BGH NJW 2013, 1441 – Morpheus).

- (19) Welche Prüfungs- und Überwachungspflichten jeweils verlangt werden können, ist eine Frage des Einzelfalls. Dafür haben sich in der Rechtsprechung in unzähligen Entscheidungen bestimmte Kriterien herausgebildet. Zu unterscheiden ist zwischen denjenigen Kriterien, die den Anbieter und das Angebot auf der einen Seite und die zur Verhinderung von Rechtsverletzungen möglicherweise zu ergreifenden Maßnahmen auf der anderen Seite betreffen. Stark verkürzt lässt sich festhalten, dass jedenfalls bei rechtmäßigen Geschäftsmodellen zu entscheiden ist, welche Maßnahmen dem Betroffenen möglich und zumutbar sind. Dabei ist im Rahmen der Zumutbarkeit für jede konkrete Maßnahme eine Abwägung der Interessen des Geschädigten, des vermittelnden Anbieters und der Allgemeinheit durchzuführen (BGH NJW 2004, 2158 (2159) – Schöner Wetten; BGH MMR 2004, 668 – Internet-Versteigerung I; BGH MMR 2007, 634 (637) – Jugendgefährdende Medien bei Ebay; BGH NJW 2013, 784 Rn. 31 – Alone in the Dark), wobei beim Angebot rechtmäßiger und von der Rechtsordnung gebilligter Geschäftsmodelle – dazu gehört das Angebot des Zugangs zum Internet und auch WLAN – die Grenze der Zumutbarkeit überschritten ist, wenn das Geschäftsmodell erheblich beeinträchtigt wird (BGH MMR 2011, 172 (173) – Kinderhochstühle im Internet; BGH MMR 2007, 634 (637) – Jugendgefährdende Medien bei Ebay; BGH NJW 2013, 784 Rn. 22 – Alone in the Dark).
- (20) Wird der Betreiber eines WLANs als Störer in Anspruch genommen, kann zusätzlich ein Anspruch auf Ersatz von Abmahnkosten bestehen. Da bisher unklar ist, ob überhaupt und welche Pflichten Access Provider (und damit WLAN-Betreiber) ergreifen müssten, besteht insoweit zusätzlich ein Risiko.

### 5. WELCHE HAFTUNGSPRIVILEGIERUNGEN SIND DE LEGE FERENDA DENKBAR?

- (21) Denkbar – und aufgrund der bestehenden Unsicherheiten auch sinnvoll – ist eine Klarstellung, wonach die Privilegierung des § 8 Abs. 1 TMG auch für Unterlassungsansprüche Anwendung findet (vgl. BT-Drs. 18/3047 sowie § 8 Abs. 3 Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes, zu diesem Entwurf eingehend *Mantz/Sassenberg*, CR 2015, 298; BR-Drs. 440/1/15).



## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

- (22) Der von der Bundesregierung verabschiedete Gesetzesentwurf zur Änderung des TMG (BR-Drs. 440/15) sieht eine solche Klarstellung vor. Nach § 8 Abs. 4 TMG-E soll die Privilegierung für Unterlassungsansprüche jedoch nur greifen, wenn die Betreiber „zumutbare Maßnahmen ergriffen haben, um eine Rechtsverletzung durch Nutzer zu verhindern“. Dabei konkretisiert § 8 Abs. 4 S. 2 TMG-E diese Maßnahmen, nämlich (i.) angemessene Sicherungsmaßnahmen gegen den unberechtigten Zugriff auf das WLAN und (ii.) Einholung einer Erklärung des Nutzers, dass dieser im Rahmen der Nutzung keine Rechtsverletzungen begehen wird. Diese Anforderungen müssen dabei kumulativ erfüllt sein, wie schon der Gesetzeswortlaut („und“) deutlich macht.
- (23) Nach der Gesetzesbegründung sollen als zumutbare Maßnahmen insbesondere die Verschlüsselung des WLANs oder die freiwillige Registrierung der Nutzer dienen. Die Verschlüsselung ist problematisch, da sie für das gesteckte Ziel nutzlos und sogar kontraproduktiv ist. Sie verhindert, dass der Nutzer einfach und unkompliziert den Zugang zum WLAN und damit zum Internet erhält, da immer zunächst ein Schlüssel ausgetauscht werden muss (*Mantz/Sassenberg*, CR 2015, 298). Diese Einschränkung gefährdet das Geschäftsmodell von öffentlichen WLANs erheblich. Denn rund 20% der Nutzer von WLANs lassen sich bereits von einfachen Hürden wie einer Vorschaltseite oder Registrierung von der Nutzung eines WLANs abhalten (Befragung Kabel Deutschland, Pressemitteilung v. 6.3.2014, <https://www.kabeldeutschland.com/de/presse/pressemitteilung/produktnachrichten/632014.html>). Es stellt ein großes Hindernis dar, dass der Nutzer zunächst an den Schlüssel kommen muss. In Restaurants und Cafés mag man den Schlüssel in die Speisekarte drucken können. In einer Vielzahl von Situationen steht dem Betreiber eine solche Möglichkeit aber nicht offen. Unklar ist z.B., wie bei WLAN-Hotspots an Bahnhöfen oder Flughäfen den Nutzern das Passwort mitgeteilt werden soll. Insbesondere ist die Verschlüsselung des WLANs nicht geeignet, Rechtsverletzungen zu verhindern. Denn jeder Nutzer, der den WPA2-Schlüssel erhält, z.B. aus der Speisekarte des Restaurants, ist in der Lage, aus dem WLAN heraus Rechtsverletzungen zu begehen. Darüber hinaus ist die Verschlüsselung auch nicht geeignet, im Falle einer Rechtsverletzung den Täter ausfindig zu machen. Eine Verschlüsselungspflicht wird zusätzlich dazu führen, dass der Großteil der in Deutschland betriebenen öffentlichen WLAN-Hotspots umgerüstet werden muss. Denn bisher war selbst bei der Mehrzahl der WLAN-Hotspots mit Registrierung der Zugang zum WLAN selbst zunächst ohne Passwort möglich. Die Anmeldung erfolgte dann (innerhalb des WLANs) auf einer sog. Splash-Page. Dementsprechend kommen auf Betreiber von WLANs Kosten für die Umrüstung sowie höhere Kosten bei der Neueinrichtung zu. Beispielsweise das von Verkehrsminister Dobrindt (CSU) erst im März 2015 vorgestellte öffentliche und barrierefreie WLAN in 100 Behördengebäuden in Bonn müsste umgerüstet werden. Wie die Benutzung anschließend wieder barrierefrei gewährleistet sein soll, bleibt ebenfalls unklar.
- (24) Als Alternative soll der Anbieter eine „freiwillige Registrierung“ vornehmen. Dies ist wohl so zu verstehen, dass der Nutzer gebeten werden soll, seine Daten einzugeben, wobei deutlich zu machen ist, dass diese Eingabe freiwillig erfolgt. Es ist davon

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

auszugehen, dass kaum Nutzer von dieser freiwilligen Möglichkeit Gebrauch machen werden, so dass auch insoweit unklar bleibt, wie diese Maßnahme Rechtsverletzungen verhindern soll.

- (25) Auch die Erklärung des Nutzers, dass er keine Rechtsverletzungen begehen werde, ist dem Ziel des Gesetzes nicht förderlich. Dabei soll das Einverständnis in eine entsprechende Klausel in AGB ausreichen. Es ist nicht zu ersehen, wie durch eine solche Erklärung Rechtsverletzungen tatsächlich verhindert werden können (*Mantz/Sassenberg*, CR 2015, 298). Es ist zweifelhaft, ob sich Nutzer, die sich zur Vornahme von Rechtsverletzungen entschlossen haben, von einem solchen – konsequenzlosen – Versprechen tatsächlich abhalten lassen werden (*Hullen*, jurisPR-ITR 7/2015, Anm. 2: „Placebo“; *Bergt*, CR-Online v. 1.3.2015, <http://www.cr-online.de/blog/2015/03/01/gesetzentwurf-zur-abschaffung-freier-wlans>). Dem folgend geht die Rechtsprechung bezüglich der Störerhaftung von jeher davon aus, dass der Täter eigenverantwortlich handelt und der Anbieter von dessen rechtskonformem Verhalten ausgehen darf (vgl. BGH GRUR 2003, 969 – Ausschreibung von Vermessungsleistungen; *Mantz*, GRUR-RR 2013, 497). Eine entsprechende Erklärung in AGB wird generell für untauglich gehalten (OLG Hamburg, Urt. v. 28.1.2009 – 5 U 255/07, NJOZ 2009, 1595 (1619) – alphasoad). Darüber hinaus sind Vorschaltseiten zwar eine praktikable Lösung, technisch aber schwierig zu realisieren. In der Regel wird der Nutzer beim Aufruf irgendeiner Webseite im WWW durch einen „Trick“ zwangsweise auf die Splash-Page umgeleitet. Erst nachdem er dort die Erklärung erteilt hat, kann er weitersurfen. Problematisch ist dies bspw., wenn der Nutzer gar kein WWW nutzt, sondern nur am Mobiltelefon die E-Mails über eine Applikation nutzen will. Er erhält keine Fehlermeldung und wird kaum verstehen, warum der Zugang zum Internet „nicht funktioniert“.
- (26) Dem folgend ist gegen den Gesetzesentwurf heftige Kritik erhoben worden (Nachweise bei *Mantz/Sassenberg*, CR 2015, 298, 305). Daraufhin hat auch der Wirtschaftsausschuss des Bundesrats eine Änderung des Gesetzesentwurfs vorgeschlagen (BR-Drs. 440/1/2015), wonach Verschlüsselung, Registrierung und Einholung einer Erklärung nicht mehr erforderlich sein sollen. Der Wirtschaftsausschuss sieht diese als hinderlich bei der Förderung und Verbreitung von WLANs an. Die von der Bundesregierung in ihrem Gesetzesentwurf herausgestellte Gefahr von Rechtsverletzungen erkennt der Wirtschaftsausschuss des Bundesrats nicht. Auch Thüringen plant einen entsprechenden Vorstoß zur Änderung des Gesetzesentwurfs im Bundesrat (Meldung bei Heise-Online v. 27.10.2015, <http://www.heise.de/newsticker/meldung/Thueringen-will-WLAN-Anbieter-ganz-von-der-Stoererhaftung-befreien-2860225.html>).

### 6. EXISTIEREN GRÜNDE, ZUKÜNFTIG ZWISCHEN PRIVATEN UND GEWERBLICHEN/INSTITUTIONELLEN BETREIBERN ZU UNTERSCHIEDEN?

- (27) Es bestehen keine Gründe, zukünftig zwischen privaten und gewerblichen/institutionellen Betreibern zu unterscheiden. Bisher war eine solche Entscheidung durch die Gerichte auch nicht thematisiert worden. Die Bundesregierung

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

hatte im ersten Entwurf zur Änderung des TMG noch eine Unterscheidung zwischen gewerblichen/institutionellen („*geschäftsmäßigen*“) und privaten („*nicht geschäftsmäßigen*“) Betreibern vorgesehen (dazu *Mantz/Sassenberg*, CR 2015, 298, 300 ff.), hat diese Unterscheidung jedoch auf die erhebliche Kritik daran fallen gelassen. Insbesondere kann von privaten Betreibern nicht mehr verlangt werden als von gewerblichen/institutionellen Betreibern. Dies hat auch der BGH in seiner Entscheidung „*Sommer unseres Lebens*“ herausgestellt (BGH MMR 2010, 565 Rn. 23 – *Sommer unseres Lebens*). Denn private Betreiber haben meist weniger Sachkenntnis und weniger wirtschaftliche Möglichkeiten.

### 7. BESTEHEN NEBEN DEN ZIVILRECHTLICHEN HAFTUNGSFRAGEN SICHERHEITSPOLITISCHE BZW. STRAFVERFOLGUNGSERHEBLICHE BEDENKEN?

- (28) E-Commerce-Richtlinie und TMG haben eine klare Haftungsregelung für Access Provider getroffen: Wer sich als Diensteanbieter neutral verhält, soll nicht für die Handlungen seiner Nutzer haften. Hierbei wird nicht zwischen „*klassischen*“ Telekommunikationsanbietern und Betreibern von offenen WLANs differenziert.
- (29) Im aktuellen Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes geht die Bundesregierung – ohne nähere Begründung – davon aus, dass mit der weiteren Verbreitung von WLANs die Gefahr von Rechtsverletzungen steigen würde, weil Nutzer darin anonym handeln könnten. Diese Auffassung verkennt, dass sich WLANs im Ergebnis nicht von anderen Mitteln zur Kommunikation unterscheiden und dass es bisher keine nennenswerten Vorfälle von Rechtsverletzungen über öffentliche WLANs gegeben hat (mabb-Stellungnahme v. 7.4.2015, [http://www.mabb.de/files/content/document/Stellungnahmen/mabb\\_Stellungnahme\\_BMWi\\_TMGAendG.pdf](http://www.mabb.de/files/content/document/Stellungnahmen/mabb_Stellungnahme_BMWi_TMGAendG.pdf), S. 3; hierauf stellt auch der Wirtschaftsausschuss des Bundesrates ab, BR-Drs. 440/1/2015, S. 4 f.). Auch bei der Nutzung von „*klassischen*“ Telekommunikationsanbietern ist eine Identifikation möglicher Rechtsverletzer nicht gewährleistet. Einige dieser Anbieter speicherten (im Einklang mit den bisherigen Bestimmungen vor Einführung der Vorratsdatenspeicherung) IP-Adressen ihrer Nutzer nicht. Nach Ende der Verbindung konnte ein bestimmter Nutzer daher nicht mehr identifiziert werden. Auch beim mobilen Internetzugang über das Mobilfunknetz (UMTS oder LTE) konnte der Täter nicht identifiziert werden. Nach Kenntnis der Verfasser hat dies bisher weder zu Problemen noch zu gesetzgeberischer Tätigkeit geführt. Es kann aber keinen Unterschied machen, ob man ein WLAN über einen Mobilfunkanschluss anbindet (sog. Tethering) oder über einen „*klassischen*“ Telekommunikationsanbieter.
- (30) Darüber hinaus hat die Bundesregierung auch im „*Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*“ (Vorratsdatenspeicherungsgesetz, BT-Drs. 18/5088) den Großteil der Betreiber von WLAN-Hotspots von der Speicherpflicht ausgenommen. So bezieht sich die Gesetzesbegründung ausdrücklich (BT-Drs. 18/5088, S. 37) auf eine Einschränkung des Verpflichtetenkreises aufgrund einer neuen Auslegung der Bundesnetzagentur des Begriffs des „Erbringens“ in ihrer Mitteilung Nr. 149/15 (hierzu auch unter B.II.2;

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

eingehend *Sassenberg/Mantz*, MMR 2015, 428). Danach sind insbesondere kleinere WLAN-Hotspots, bei denen zur Erbringung ein vorhandene DSL-Anschluss genutzt sowie den Nutzern nur für kurze Zeit und nicht dauerhaft und mittels einer festen IP-Adresse der Zugang zum Internet gewährt wird, nicht als Erbringer von Telekommunikationsdiensten anzusehen. In der Gesetzesbegründung heißt es (BT-Drs. 18/5088, S. 37):

*„Nicht verpflichtet sind demnach Anbieter, die ihren Kunden nur eine kurzzeitige Nutzung des Telekommunikationsanschlusses ermöglichen, zum Beispiel Betreiber von Hotels, Restaurants und Cafés, die ihren Kunden eine Telefon- oder Internetnutzung zur Verfügung stellen...“*

- (31) Weiter sind insbesondere Verletzungen von gewerblichen Schutzrechten nach dem neu gefassten § 100g Abs. 2 StPO nicht als „*besonders schwere Rechtsverletzungen*“ anzusehen, die eine Beauskunftung der durch die Vorratsdatenspeicherung erhobenen und gespeicherten Daten erlauben würde.

### **8. WIE IST DIE STRAFRECHTLICHE VERANTWORTLICHKEIT VON BETREIBERN OFFENER WLAN-NETZE EINZUORDNEN IM HINBLICK AUF BEIHILFE, MITTÄTERSCHAFT UND (EVENTUAL-)VORSATZ?**

- (32) Wie oben dargestellt, sind Betreiber von WLAN-Hotspots nach § 8 Abs. 1 TMG privilegiert. Unter den Voraussetzungen der Norm ist eine strafrechtliche Verantwortlichkeit ausgeschlossen. Solange sich der WLAN-Betreiber daher im Hinblick auf die übermittelten Informationen neutral verhält und diese lediglich durchleitet, handelt er weder als Mittäter noch als Beihelfer.
- (33) Darüber hinaus hat der WLAN-Betreiber aufgrund seiner neutralen Stellung auch keinen Vorsatz hinsichtlich eventueller rechtswidriger Taten seiner Nutzer. Dies gilt auch im Hinblick auf die Annahme eines Eventualvorsatzes. Solange der Betreiber keine konkrete Kenntnis von konkreten rechtswidrigen Handlungen seiner Nutzer hat oder mit diesen im Sinne von § 8 Abs. 1 S. 2 TMG kollusiv zusammenwirkt, liegt ein Eventualvorsatz nicht vor. Ein solcher ist auch dann nicht anzunehmen, wenn der Betreiber sich grundsätzlich bewusst ist, dass über das Netzwerk rechtswidrige Handlungen begangen werden können. Im Hinblick auf Host Provider ist in der Rechtsprechung bei der hartnäckigen Weigerung der Löschung rechtsverletzender Inhalte teilweise eine Gehilfenhaftung angenommen worden (OLG Hamburg GRUR-RR 2013, 382; LG Frankfurt, Urt. v. 05.02.2014 - 2-06 O 319/13, BeckRS 2014, 03623). Diese Rechtsprechung soll – für Host Provider – nach dem Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (BR-Drs. 440/15) in § 10 TMG-E kodifiziert werden. Auf den Access Provider oder den WLAN-Betreiber ist dies aus den oben aufgeführten Gründen nicht übertragbar, was auch die im Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes klare Unterscheidung zwischen dem Access Provider und dem Host Provider erneut deutlich macht.

# Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

## II. DATENSCHUTZ UND DATENSICHERHEIT

### 1. AUS WELCHEN GRÜNDEN IST ES SINNVOLL/NICHT SINNVOLL HAFTUNGSPRIVILEGIERUNGEN NUR FÜR VERSCHLÜSSELTE VERBINDUNGEN VORZUSEHEN?

- (34) Die Verschlüsselung einer Verbindung darf nicht mit dem Erfordernis einer Nutzeridentifikation gleichgesetzt werden. Einer solchen Nutzeridentifikation bedarf es gerade nicht, um eine Verschlüsselung des Verkehrs zu erreichen. Durch eine Verschlüsselung der Verbindung soll und kann vielmehr alleine verhindert werden, dass Dritte den Verkehr ohne größere technische Anstrengung „mitlesen“ können. Es steht zu befürchten, dass eine Verschlüsselung eine unnötige zusätzliche Hürde für Nutzer und Betreiber darstellt, diese zudem nur geringfügig zur Absicherung gegenüber dem Zugriff Dritter beitragen würde und für die Betreiber zusätzliche Kosten entstehen (hierzu auch unter B.I.4, ausführlich: *Mantz/Sassenberg*, CR 2015, 298 (301 f.)). Insofern läuft eine Verschlüsselung dem Interesse der Förderung von freien WLAN-Hotspots entgegen. Ein Zusammenhang mit der Frage einer Haftungsprivilegierung ist nicht zu erkennen.

### 2. BEDARF ES TECHNISCHER AUFLAGEN FÜR DEN BETRIEB ZUR GEWÄHRUNG VON DATENSCHUTZ- UND DATENSICHERHEIT? GIBT ES ALLGEMEINE STANDARDS?

- (35) De lege lata sind gesetzliche Regelungen für Datenschutz- und Datensicherheit vorgesehen, welche von einem Betreiber eines offenen WLANs zu berücksichtigen sind. Ausschlaggebend sind insofern die telekommunikationsrechtlichen Bestimmungen, nicht einschlägig sind hingegen die Vorgaben des TMG. Die regulatorischen Bestimmungen des Telekommunikationsgesetzes (TKG) unterscheiden hierbei zwischen verschiedenen Adressaten, an die sich die jeweiligen Regelungen wenden. Auf der einen Seite ist die Bejahung der Diensteanbiereigenschaft, auf der anderen Seite der Eigenschaft als Anbieter von öffentlich zugänglichen Telekommunikationsdiensten und Betreiber öffentlicher Telekommunikationsnetze entscheidend.

#### a. Diensteanbieter

- (36) Alle Anbieter von offenen bzw. öffentlichen WLANs sind als Diensteanbieter nach § 3 Nr. 6 TKG anzusehen (*Redeker*, ITRB 2011, 186 (186 f.); zu Hotels vgl. *Ricke* in *Spindler/Schuster*, Recht der elektronischen Medien, 3. Aufl. 2015, § 3 TKG Rn. 9; *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 34 ff. m.w.N.). Diensteanbieter ist „jeder, der ganz oder teilweise geschäftsmäßig a) Telekommunikationsdienste erbringt oder b) an der Erbringung solcher Dienste mitwirkt“. Bereits das Mitwirken an der Erbringung eines Dienstes ist damit ausreichend, wobei das Mitwirken Aufgaben betreffen muss, die mit der charakteristischen Signalübertragung und deren insbesondere datenschutzrechtlichen Gefahren in Zusammenhang stehen (vgl. *Sassenberg/Franke*, CR 2013, 772 (775)). Unter dem Merkmal des geschäftsmäßigen Erbringens von Telekommunikationsdiensten wird gemäß § 3 Nr. 10 TKG das „nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

*Gewinnerzielungsabsicht*“ verstanden. Die Bejahung der Eigenschaft als Diensteanbieter hat zur Folge, dass die Regelungen zum Fernmeldegeheimnis (§§ 88 ff. TKG), zum telekommunikationsrechtlichen Datenschutz (§§ 91 ff. TKG) sowie ein Teil der Regelungen zur öffentlichen Sicherheit (§§ 108 ff. TKG) zur Anwendung kommen.

- (37) Der Diensteanbieter unterliegt dem Fernmeldegeheimnis nach § 88 TKG, wobei Verstöße nach § 206 StGB strafbewehrt sind. Die datenschutzrechtlichen Regelungen ergeben sich aus den §§ 91 ff. TKG, die den Umgang mit personenbezogenen Daten, insbesondere also mit Bestands- und Verkehrsdaten, regeln. Hinsichtlich des (restriktiven) Umgangs mit Verkehrsdaten haben die Bundesbeauftragte für Datenschutz und Informationssicherheit (BfDI) und die Bundesnetzagentur (BNetzA) am 19.12.2012 einen Leitfaden herausgegeben, in den sich auch die einzelnen Betreibermodelle einordnen lassen.
- (38) Der Diensteanbieter unterliegt jedoch nicht nur dem Fernmeldegeheimnis und muss die Bestimmungen des telekommunikationsrechtlichen Datenschutzes einhalten. Er muss nach § 109 Abs. 1 TKG auch die erforderlichen technischen Vorkehrungen und sonstigen Maßnahmen treffen, die zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten erforderlich sind. So sollen Fernmeldegeheimnis und Datenschutz sowie der Betrieb im Katastrophenfall sichergestellt werden. Konkrete Anforderungen, welche technischen Vorkehrungen und Maßnahmen zu ergreifen sind, hat der Gesetzgeber nicht vorgesehen, so dass der Diensteanbieter die im konkreten Fall erforderlichen technischen Vorkehrungen und sonstige Maßnahmen ermitteln muss. Die BNetzA hat zudem im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und der BfDI einen Katalog von Sicherheitsanforderungen gem. § 109 Abs. 6 TKG erstellt, der Anbietern als Grundlage zur Erfüllung der gesetzlichen Verpflichtung dienen soll. Der Entwurf einer aktualisierten Fassung wurde gerade im Amtsblatt der Bundesnetzagentur (ABl. Nr. 19/2015 unter der Mitteilungs-Nr. 1213/2015) veröffentlicht. Welche Maßnahmen im Einzelfall zu treffen sind, hängt vom jeweiligen Betreibermodell ab. Ausschlaggebend ist hierbei auch, ob Bestandsdaten erhoben werden. Hinsichtlich der technischen Vorkehrungen liefern die IT-Grundschutzkataloge des BSI einen Anhaltspunkt.

### **b. Anbieter von öffentlich zugänglichen Telekommunikationsdiensten und Betreiber öffentlicher Telekommunikationsnetze**

- (39) Zudem ist der Betreiber eines offenen WLANs als Anbieter von öffentlich zugänglichen Telekommunikationsdiensten anzusehen (vgl. *Sassenberg/Mantz*, WLAN und Recht, 2014, Rn. 22 ff. m.w.N.). Seitens der BNetzA wird entgegen der bisher einhelligen Literaturauffassung danach differenziert, ob durch den Anbieter ein eigener, in der Regel auf eine bestimmte Dauer angelegter Telekommunikationsanschluss überlassen wird oder lediglich die Nutzung eines vorhandenen TK-Anschlusses erfolgt (vgl. Mitteilung 149/2015 der Bundesnetzagentur, ABl. 4/2015 vom 04.03.2015, S. 1140). Nur wenn ein eigener Telekommunikationsanschluss überlassen wird, liegt

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

danach ein Fall des „Erbringens“ von Telekommunikationsdiensten vor. Wird jedoch ein vorhandener DSL-Anschluss genutzt, so liegt kein Fall des „Erbringens“ sondern lediglich ein „Mitwirken“ vor, das für die Anbietereigenschaft nicht ausreichend sei. Die Auffassung der Bundesnetzagentur reduziert die regulatorischen Anforderungen für kleinere Hotspot-Betreiber und ist insoweit hinsichtlich des Ergebnisses zu begrüßen, gleichwohl vermag die Ungleichbehandlung der Anbieter jedoch dogmatisch nicht zu überzeugen und lässt zudem unberücksichtigt, dass auch das Betreiben von öffentlichen Telekommunikationsnetzen die regulatorischen Pflichten auslöst (hierzu im Einzelnen *Sassenberg/Mantz*, MMR 2015, 428 ff.).

- (40) Wird für den jeweiligen WLAN-Hotspot die Anbieter- und/oder Betreibereigenschaft angenommen, so ist die Folge, dass nicht nur die Kundenschutzvorschriften in §§ 43 a ff. TKG grundsätzlich anwendbar sind, sondern dass auch weitere Anforderungen der öffentlichen Sicherheit (§§ 108 ff. TKG) zur Anwendung kommen, nämlich insbesondere ein Sicherheitsbeauftragter zu benennen und ein Sicherheitskonzept zu erstellen ist. Bei Datenschutzverstößen besteht – unabhängig von deren Schweregrad – eine Meldepflicht nach § 109a TKG bzw. der EU-Verordnung 611/2013 „über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG.“

### c. Keine (weiteren) technischen Auflagen erforderlich

- (41) Die obigen Ausführungen zeigen, dass durch die bestehenden rechtlichen Rahmenbedingungen die Gewährung von Datenschutz- und Datensicherheit bereits hinreichend sichergestellt ist. Die Bandbreite unterschiedlicher Betreibermodelle trägt dazu bei, dass eine konkretere Regelung nur wenig erfolgversprechend wäre. Die Frage, ob es zusätzlicher technischer Auflagen für Betreiber von „öffentlichen WLAN-Hotspots“ bedarf, ist daher zu verneinen. Vielmehr stellen bereits die existierenden Regelungen Datenschutz- und Datensicherheit in einem ausreichenden Maße sicher. Aufgrund der abstrakten gesetzlichen Regelungen besteht die Gefahr, dass gerade kleinere Anbieter mit der Umsetzung der diesbezüglichen Anforderungen überfordert sind und diese daher der Verbreitung von freien WLAN-Hotspots entgegenstehen. Werden jedoch keine Bestandsdaten erhoben und die Verbindungsdaten unmittelbar mit der Beendigung der Verbindung gelöscht, so ergeben sich aus den Regelungen zur öffentlichen Sicherheit de facto nur geringe Anforderungen. Dem Stellenwert des Fernmeldegeheimnisses sowie des Datenschutzes wird insoweit in Abhängigkeit vom jeweiligen Betreibermodell Rechnung getragen, so dass von einem ausgewogenen rechtlichen Rahmen auszugehen ist.

### III. INTERNATIONALER VERGLEICH

#### 1. IN WELCHEM RECHTLICHEN RAHMEN IM HINBLICK AUF ZIVIL- UND STRAFRECHTLICHE ASPEKTE OPERIEREN WLAN-BETREIBER IM INTERNATIONALEN VERGLEICH?

- (42) Seitens des eco – Verbands der deutschen Internetwirtschaft e.V. (eco) wurde im November 2014 eine Studie zur „*Verbreitung und Nutzung von WLAN, WLAN-Zugangspunkten sowie öffentlichen Hotspots in Deutschland*“ durchgeführt. Im Rahmen der Studie wird vom eco aufgezeigt, dass die Verbreitung von freien öffentlichen WLAN-Hotspots im internationalen Vergleich gering ist und Länder wie Südkorea, Großbritannien, Taiwan, Schweden, Frankreich und die USA über eine erheblich größere Reichweite verfügen. Auch in Estland können fast überall freie WLAN-Hotspots genutzt werden (*Grüner*, golem.de Beitrag „WLAN-Paradies Estland“ vom 16.07.2012).
- (43) Die Frage der Verantwortlichkeit speziell des WLAN-Betreibers ist innerhalb Europas nicht harmonisiert. Die Mitgliedsstaaten sind – im Rahmen der Vorgaben der E-Commerce-Richtlinie – in der Ausgestaltung der Haftung von Intermediären frei (Erwägungsgrund 59 der E-Commerce-Richtlinie). Die in den Mitgliedsstaaten anzutreffenden Regelungsmodelle zur Verantwortlichkeit sind sehr unterschiedlich und abweichend zur deutschen Störerhaftung geregelt, wenngleich es Ähnlichkeiten in der Rechtsprechung gibt (vgl. *Ohly*, ZUM 2013, 308 (311 m.w.N.); *Lensing-Kramer*, GRUR 2009, 722 (724)). Die Frage der Haftung des Betreibers öffentlicher WLANs wird – soweit ersichtlich – hauptsächlich in Deutschland diskutiert.

#### 2. WELCHE ERKENNTNISSE LASSEN SICH HIERAUS FÜR DEUTSCHLAND UND HESSEN ABLEITEN?

- (44) Für den im Vergleich zögerlichen Ausbau in Deutschland werden regelmäßig die regulatorischen Bestimmungen des Telekommunikationsrechts sowie die Gefahr der Verantwortlichkeit des Hotspot-Betreibers für ein Handeln Dritter angeführt, wobei der letzte Punkt klar die Diskussion beherrscht. Die anhaltende Unsicherheit über den Rechtsrahmen und die daraus resultierende zögerliche Herangehensweise werden dabei inzwischen kurz als „*German Angst*“ zusammengefasst und führten zu der (überzogenen bzw. plakativen) Forderung, die Störerhaftung generell „abzuschaffen“. Die international bestehenden unterschiedlichen Regelungsmodelle sollten nicht dazu führen, dass die Störerhaftung bzw. Täterhaftung wegen Verkehrspflichtverletzung grundsätzlich in Frage gestellt wird. Diese hat sich vielmehr als effektiv und flexibel erwiesen (*Ohly*, ZUM 2013, 308 (312 f.)). Unabhängig von der Frage, ob langfristig eine europäische Vollharmonisierung wünschenswert wäre, geht es derzeit darum, national zu klären, ob und wenn ja, welche Prüfungs- und Verkehrspflichten für Betreiber von WLAN-Hotspots bestehen. Diese Konkretisierung kann dabei – natürlich nur unter Berücksichtigung des europäischen Rechtsrahmens – sowohl durch den Gesetzgeber als auch durch die Rechtsprechung erfolgen. Richtigerweise haben CDU, CSU und SPD im Koalitionsvertrag vom 16.12.2013 daher auch „nur“ davon



## **Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“**

gesprochen, dass für offene WLANs eine „Klarstellung der Haftungsregelungen“ erfolgen soll. Der internationale Vergleich bestätigt, dass es aus dem Gesichtspunkt der Rechtssicherheit nicht erforderlich ist, dem Hotspot-Betreiber Prüfungs- und Verkehrspflichten aufzuerlegen.

### **IV. AUSBAU**

#### **1. WELCHE GRÜNDE SPRECHEN FÜR UND GEGEN ÖFFENTLICHE FÖRDERUNG BEI AUFBAU UND/ODER BETRIEB VON WLAN-NETZEN?**

- (45) Die im internationalen Vergleich geringe Verbreitung (siehe hierzu unter B.III.1) spricht für eine Förderung von öffentlichen WLANs. Die Förderung könnte – auch wenn der geringe Ausbaustand primär auf die Rechtsunsicherheit und regulatorischen Anforderungen zurückzuführen ist – dazu beitragen, dass der im Vergleich zu anderen Ländern bestehende Rückstand so schnell wie möglich aufgeholt wird. Hiervon würde nicht nur die Wirtschaft, beispielsweise in Form der Förderung des Tourismus oder der Möglichkeit des mobilen Arbeitens, profitieren. Vielfach würde auch der mobile Informationsaustausch gefördert. Es ist nicht davon auszugehen, dass sich eine solche Förderung auf Anbieter von Festnetz- oder Mobilfunkprodukten negativ auswirken würde (siehe hierzu unter B.IV.5). Bei der Förderung ist allerdings unter Berücksichtigung des Grundsatzes der Gleichbehandlung darauf zu achten, dass keine negativen Effekte für Geschäftsmodelle von entgeltpflichtigen WLAN-Betreibern entstehen.

#### **2. WELCHE INSTRUMENTE DER FÖRDERUNG EXISTIEREN? WELCHE SIND IHNEN BEKANNT? WELCHE FORMEN DER FÖRDERUNG WÄREN DENKBAR?**

- (46) Gerade beim Aufbau von städtischen WLANs hat sich gezeigt, dass der Verfügbarkeit von zentralen Standpunkten für den Aufbau der Router sowie der Infrastruktur (Strom, Anbindung ans Internet) an sich eine wesentliche Bedeutung zukommt. Die öffentliche Hand verfügt in der Regel über innerstädtische Gebäude, die für den Aufbau eines innerstädtischen Netzes genutzt werden können. Der Ausbau kann insofern nicht nur mit finanziellen Mitteln zur Verfügung gefördert werden, sondern auch mit der Bereitstellung der vorhandenen Infrastruktur. Teilweise wird die Förderung davon abhängig gemacht, dass der Anbieter zumindest für einen bestimmten Zeitraum – z.B. 30 Minuten am Tag – einen kostenlosen Zugang für Jedermann gewährleistet.
- (47) Theoretisch wäre auch ein eigener Betrieb durch die öffentliche Hand zur Förderung der Verbreitung von WLANs denkbar, wobei hier zu berücksichtigen ist, dass die Erbringung von Telekommunikationsdienstleistungen aufgrund der landes- und verfassungsrechtlichen Rahmenbedingungen nur in einem engen Rahmen zulässig ist (*Sassenberg/Mantz, WLAN und Recht, 2014, Rn. 345 ff.*).

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

### 3. WELCHE BETREIBERMODELLE EXISTIEREN? WELCHE MODELLE WERDEN AM HÄUFIGSTEN GEWÄHLT UND WIE KANN MAN DIES ERKLÄREN?

- (48) Die nachfolgende Übersicht zeigt die gängigen Betreibermodelle für offene WLANs auf und beschreibt diese summarisch, eine ausführliche Darstellung der Betreibermodelle findet sich bei *Sassenberg/Mantz, WLAN und Recht, 2014, Rn. 11 ff.*:

Betreibermodell	Beschreibung
WLAN zur Absatzförderung	Der Aufbau und Betrieb eines WLANs wird zur Förderung des Absatzes der eigenen Leistungen genutzt (z.B. Café, Hotel oder Kaufhaus).
Werbefinanziertes WLAN	Der Aufbau und Betrieb eines WLANs wird durch Werbung finanziert.
Kommunales WLAN	Der Aufbau und Betrieb eines WLANs erfolgt durch die öffentliche Hand.
Freies WLAN	Der Aufbau und Betrieb eines WLANs erfolgt aus altruistischen Gründen.
Entgeltpflichtiges WLAN	Die Nutzung des WLANs ist entgeltpflichtig.
Kommerzielles WLAN-Sharing	Ein Anbieter nutzt vorhandene – in der Regel eigene – Infrastruktur (z.B. in Form eines DSL oder Kabelanschlusses) um nicht nur einen Kunden anzubinden, sondern mit den nicht benötigten Kapazitäten ein WLAN-Netzwerk aufzubauen. Betreiber des Hotspots ist der Anbieter.

- (49) Auch sind Abweichungen von den vorgestellten Betreibermodellen zu finden bzw. diese werden zum Teil kombiniert (z.B. entgeltfreie Nutzung nur für 30 Minuten). Allgemein lässt sich sagen, dass sämtliche Betreibermodelle anzutreffen sind. Die weiteste Verbreitung dürften hierbei WLANs zur Absatzförderung haben. Dies lässt sich damit begründen, dass Kunden den kostenlosen Internetzugang inzwischen zum Gegenstand für ihre Auswahlentscheidung machen (hierzu bereits unter B.V.2). Darauf dürften entgeltliche WLANs folgen.

### 4. WELCHE ROLLE KANN DAS MODELL „FREIFUNK“ FÜR DEN AUSBAU DES WLAN IN HESSEN SPIELEN?

- (50) Verteilt über Deutschland existieren viele WLAN-Hotspots, die nach dem sog. Freifunk-Modell von Privaten angeboten werden. Die Freifunk-Communities in Hessen waren in den letzten Jahren sehr aktiv und zeichnen sich durch ein stetes Wachstum aus. Nach Kenntnis der Verfasser bestehen u.a. Kontakte zur Stadt Frankfurt am Main. Freifunk-Communities in Deutschland und speziell auch in Hessen und Frankfurt statten zudem bereits aktiv neu eingerichtete Flüchtlingsunterkünfte mit WLAN aus, wo dies aufgrund der jeweiligen Gegebenheiten möglich ist.

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

- (51) Freifunk kann für den Aufbau von öffentlichen Hotspots daher verschiedene Rollen einnehmen. Zum einen stellen diese bereits heute, wenn auch teils noch weit verteilt oder nicht großflächig, öffentlich zugängliche, freie WLAN-Hotspots zur Verfügung. Es gibt eine Vielzahl an Beispielen der Zusammenarbeit von Gemeinden mit Freifunk-Communities, die zum kostengünstigen Aufbau von WLAN-Hotspots und WLAN-Infrastruktur geführt haben. Eine Zusammenarbeit mit Freifunk kann daher den einfachen, günstigen und zudem besonders schnellen Aufbau von WLAN-Hotspots fördern. Die Umsetzung ist dabei sehr von den einzelnen Beteiligten abhängig, erfolgt in der Regel aber deutlich schneller als durch Unternehmen. Dabei bedarf es nicht zwingend einer finanziellen Förderung. Bereits die Gewährung von Zugang zu öffentlichen Gebäuden, die Übernahme von (eher geringen) Stromkosten für WLAN-Router und ggf. die Bereitstellung von Uplinks sind für den Aufbau von Freifunk-Knoten hilfreich. Des Weiteren können Mitglieder der Freifunk-Community aufgrund ihrer jahrelangen Erfahrungen Ansprechpartner darstellen.
- (52) Alternativ können vom Land Hessen oder Städten und Gemeinden aufgebaute WLAN-Hotspots auch unabhängig von Freifunk betrieben werden, wobei sich die Angebote dann – jedenfalls in der Fläche – ergänzen. Nach Kenntnis der Verfasser ist bei verschiedenen WLAN-Projekten eine Zusammenarbeit mit Freifunk auch allein dadurch erfolgt, dass eine Verbindung mit Freifunk-Knoten erfolgte. Über die Infrastruktur des öffentlichen WLANs konnten dann verteilte Freifunk-Standorte verbunden werden. Dies fördert das Zusammenwachsen der Freifunk-Netze und befördert dadurch den Aufbau neuer Knoten.
- 5. WELCHE GRÜNDE SPRECHEN FÜR EINE ZUSAMMENARBEIT DER KOMMUNEN, DER STÄDTE, DER LANDKREISE UND DES ÖPNV BEIM AUFBAU EINES ÖFFENTLICHEN WLANS? WELCHE GRÜNDE SPRECHEN DAGEGEN?**
- (53) Verschiedene Studien zeigen, dass die mobil abgerufenen Datenmengen – auch aufgrund deren rapider Zunahme – noch nicht alleine über die Mobilfunknetze übertragen werden können (vgl. Goldmedia Trendmonitor 2013, [www.goldmedia.com/aktuelles/trendmonitor-2013/data-offloading.html](http://www.goldmedia.com/aktuelles/trendmonitor-2013/data-offloading.html); Cisco, [www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white\\_paper\\_c11-520862.html](http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html)). Auch wenn die Frage der verfügbaren Bandbreite im Fokus steht, ist die WLAN-Nutzung auch aufgrund mangelnder Netzabdeckung von Interesse. Daher sollen aus Sicht der Telekommunikationsunternehmen Datenströme stattdessen über lokale WLANs übertragen werden (sog. „Data Offloading“). Auch die EU-Kommission hat dieses Potential erkannt (Entwurf der Digital Single Market-VO, COM (2013) 627 final, ErwGr. 26 f.; dazu eingehend Mantz/Sassenberg, CR 2014, 370). So wirbt bspw. der Anbieter *Telefónica* derzeit mit einem neuen Angebot, welches das Führen von Mobilfunkgesprächen über einen beliebigen WLAN-Hotspot ermöglicht und so gerade bei eingeschränktem Mobilfunkempfang eine Alternative darstellt. Neben der grundsätzlichen Frage des Netzausbaus können auch die äußeren Rahmenbedingungen – bspw. im Zug – für die Nutzung eines WLAN-Hotspots sprechen. WLAN-Angebote sind jedoch nicht nur erforderlich, um ein mobiles Arbeiten

## **Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“**

zu ermöglichen, sondern stellen gerade in den Städten auch einen Mehrwert für Touristen und Einwohner dar.

- (54) Offene WLAN-Hotspots sind weder ein Surrogat für den Internetzugang über den klassischen Telefonanschluss noch den mobilen Datentarif, so dass nicht davon auszugehen ist, dass der diesbezügliche Wettbewerb negativ beeinträchtigt werden könnte. Dies zeigen auch die derzeit über das Mobilfunknetz übertragenen Datenmengen. So hat das pro SIM-Karte übertragene Datenvolumen im letzten Jahr zwar um 30,4% zugenommen, beläuft sich derzeit aber dennoch nur auf 377 MB pro Monat (vgl. DIALOG Consult / VATM 17 TK-Marktstudie 2015, 28). Gleichzeitig sprechen die o.g. Gründe für einen kurzfristigen Ausbau von freien WLAN-Hotspots. Hierzu kann die öffentliche Hand insbesondere auch mit den in Innenstadtlagen vorhandenen Standorten beitragen.

### **6. WER TRÄGT DIE KOSTEN FÜR DEN AUFBAU UND DEN BETRIEB VON WLAN-NETZEN?**

- (55) Der Aufbau und Betrieb von WLAN-Netzen erfolgt aus gänzlich unterschiedlichen Gründen (vgl. zu den Betreibermodellen *Sassenberg/Mantz, WLAN und Recht, 2014, Rn. 11 ff.*). Allgemein lässt sich sagen, dass der Aufbau und Betrieb in der Regel vom Betreiber des jeweiligen Netzes getragen wird. Bei entgeltfreien Angeboten geschehen Aufbau und Betrieb häufig zum Zwecke der Absatzförderung (z.B. in einem Café, Hotel oder Kaufhaus). Gerade größere Unternehmen treten hierbei jedoch aus den unter B.II.3 ausgeführten Gründen häufig nur als „Sponsor“ auf und der Betrieb erfolgt durch einen klassischen Telekommunikationsanbieter.

## **V. WIRTSCHAFTLICHE BEDEUTUNG UND EFFEKTE**

### **1. WELCHEN NUTZEN HABEN STÄDTE UND GEMEINDEN DURCH FREIE ÖFFENTLICH ZUGÄNGLICHE WLAN-NETZE?**

- (56) Für Städte und Gemeinden bieten WLAN-Hotspots verschiedene Vorteile. So können WLAN-Hotspots u.a. in öffentlichen Gebäuden zum Beispiel zur Versorgung von Wartenden dienen. Weiter können öffentliche Dienstleistungen und Echtzeitinformationen über WLANs angeboten werden, wie z. B. im öffentlichen Verkehr oder im Verkehrsmanagement. Dies hebt beispielsweise die EU-Kommission hervor. Sie hat im Entwurf zur Digital Single Market ausgeführt (COM (2013) 627 final, ErwGr 28):

*„Behörden und Anbieter öffentlicher Dienste nutzen Funk-LAN-Zugangspunkte zunehmend in ihren Räumlichkeiten für eigene Zwecke, z. B. für ihre Mitarbeiter oder um Bürgerinnen und Bürgern vor Ort einen kostengünstigen Zugang zu elektronischen Behördendiensten zu bieten, um intelligente öffentliche Dienstleistungen zu unterstützen, die die Übermittlung von Informationen in Echtzeit beinhalten, wie z. B. im öffentlichen Verkehr oder im Verkehrsmanagement. Solche Einrichtungen könnten Bürgerinnen und Bürgern*

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

*als Nebenleistung zu den in den betreffenden Räumlichkeiten angebotenen Diensten auch generell Zugang zu solchen Zugangspunkten gewähren (...)*

### **2. HABEN FREIE ÖFFENTLICH ZUGÄNGLICHE WLAN-NETZE AUCH FÜR DIE TOURISMUSWIRTSCHAFT EINE BEDEUTUNG?**

- (57) Öffentlich zugängliche WLANs haben für die Tourismuswirtschaft einen positiven Effekt. Für Hotelgäste ist die Verfügbarkeit eines WLAN mittlerweile sogar eines der wichtigsten Kriterien bei der Hotelwahl (vgl. Stellungnahme der DeHoGa/IHA zur Anhörung im Landtag Nordrhein-Westfalen v. 3.7.2013, <http://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument?Id=MMST16/933>; Pressemitteilung HRS v. 3.4.2014, <http://hrs.de/presse/pressemitteilungen/mit-gratis-wlan-auf-dem-zimmer-punkten-hotels.html>).
- (58) Verschiedene Städte nutzen öffentliche WLANs auch als Informationsplattform für Touristen, durch die Nutzern Hinweise zu Sehenswürdigkeiten, Aktionen etc. an die Hand gegeben werden.
- (59) Weiter werden Städte, die mit öffentlichen WLANs ausgestattet sind, als weltoffener und moderner wahrgenommen. Öffentliche WLANs steigern daher generell die Attraktivität von Städten und Regionen. Aus diesem Grunde werben auch Touristeninformationen mit der Verfügbarkeit von öffentlichen WLANs (so z.B. die Hamburg Tourismus GmbH, <http://www.hamburg-tourism.de/infos/mobile-angebote/wlan-hotspots>). Teilweise wird WLAN auch als Teil einer Gesamtstrategie angesehen. So schreibt der Tourismusverband Sächsisches Elbland e.V. in seiner „Destinationsstrategie“ (2. Aufl. 2014, [http://www.elbland.de/fileadmin/userfiles/TVSE/Downloads/Destinationsstrategie\\_ab\\_2014\\_Internet.pdf](http://www.elbland.de/fileadmin/userfiles/TVSE/Downloads/Destinationsstrategie_ab_2014_Internet.pdf)):

#### *„2.1.5 Digitale Versorgung*

*Die gesellschaftliche Bedeutung des Internets wächst zunehmend. Immer mehr Menschen greifen mehrmals täglich auf das World Wide Web zu. Um auch das vielfältige touristische Online-Angebot optimal zu nutzen braucht es eine schnelle Verbindung. (..)*

*WLAN-Verbindungen an touristischen Einrichtungen sollen die Ansprüche und den Bedarf der Besucher des Freistaats aus dem In- und Ausland erfüllen. Sachsen ist Kulturreiseland Nr. 1 und soll sich z.B. durch die Einrichtung von Hot Spots und WLAN an den entsprechenden Orten als modernes Reiseziel präsentieren. (...)*

*Vor allem internationale Besucher erwarten permanent verfügbares Internet, für viele stellt dies eine Buchungsvoraussetzung dar. Der Ausbau und die Weiterentwicklung des (teilweise vorhandenen) Angebotes sind für die touristischen Leistungsträger wünschenswert. So könnten z. B. (kostenfreies) WLAN in den Beherbergungen, gastronomischen Betrieben, Museen etc. noch*

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

*mehr Gäste anziehen. Auch andere elektronische Dienste vor Ort, wie z. B. Apps zu Museumsrundgängen und Stadtführungen oder GPS-gestützte Fahrradtouren hätten somit größeres Potenzial der Gästeakzeptanz (kürzere Ladezeiten etc.) (...)*“

- (60) Die Wahrnehmung von Städten und Touristenregionen wird maßgeblich auch durch die Touristen selbst geprägt. Das zeitnahe Versenden oder Posten von Fotos von Sehenswürdigkeiten oder sog. „Selfies“ ist heutzutage üblich. Besucher, die ihre Fotos unmittelbar mit Freunden oder öffentlich teilen (können), bewirken dementsprechend einen Werbeeffect (teilweise bezeichnet als „virales Marketing“). Insbesondere Skigebiete haben WLAN als Werbepattform schon vor Jahren entdeckt (vgl. <http://stadt-bremerhaven.de/wie-man-kostenloses-wlan-fuer-den-tourismus-nutzt/>). Da insbesondere ausländische Touristen sehr häufig keine Mobilfunkanbindung haben werden, sind diese auf WLANs angewiesen. So schreibt z.B. das Reiseunternehmen Thomas Cook (Eintrag v. 11.12.2014, <http://www.thomascook.de/unternehmen/newsroom/braggie-neuer-tourismus-trend-im-social-web>):

*„Mit welchen Fotos machen die Urlauber die Daheimgebliebenen am liebsten neidisch?*

*Martin Widenka: 'Mit Fotos vom Hotelbett mit direktem Blick aufs Meer, mit Cocktails beim Sonnenuntergang und tollen Bildern am Pool. Weil am liebsten sofort gepostet wird, ist besonders jungen Urlaubern kostenloses WLAN in der Hotelanlage sehr wichtig.'*“

### 3. WELCHEN NUTZEN HABEN ANDERE WIRTSCHAFTSSEKTOREN UND BRANCHEN DURCH FREI ÖFFENTLICH ZUGÄNGLICHE WLAN-NETZE?

- (61) Einen bekanntermaßen enormen Nutzen haben **Telekommunikationsunternehmen**. Diese begreifen WLAN-Hotspots als Möglichkeit zur Entlastung ihrer Mobilfunknetze. Aufgrund des ständig wachsenden Übertragungsvolumens werden auch in der näheren Zukunft die Mobilfunknetze nicht in der Lage sein, für alle Nutzer ausreichend Bandbreite zur Verfügung zu stellen (siehe oben Rn. 56).
- (62) Kostenlose WLANs haben darüber hinaus für praktisch alle Branchen einen starken Kundenbindungseffekt. Dies hat insbesondere die **Gastronomie** früh erkannt und bietet seit Jahren lokale WLANs an. Dadurch können neue Kunden angelockt und die Verweildauer der Kunden erhöht werden.
- (63) **Fernbusse** bieten bereits seit längerer Zeit kostenloses WLAN an und stellen damit gegenüber dem – derzeit noch kostenpflichtigen – nur wenig verbreiteten WLAN in der Bahn ein Unterscheidungsmerkmal und damit einen Wettbewerbsvorteil dar.
- (64) Für den **Einzelhandel** bieten WLAN-Hotspots ebenfalls die Möglichkeit, das Geschäft oder den Einkaufsbereich attraktiver zu gestalten. Über WLANs können Unternehmen auch Zusatzangebote machen. So bietet seit einigen Monaten eine deutsche

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

Drogeriekette kostenlose WLANs an. Zusätzlich können Kunden über dieses WLAN unmittelbar Dienste des Unternehmens (z.B. Foto-Entwicklung) in Anspruch nehmen.

- (65) Das Angebot eines kostenlosen WLANs führt darüber hinaus generell zu Werbeeffekten. Wer ein kostenloses WLAN anbietet, zeigt dem Kunden, dass er mit der Zeit zu gehen weiß. Über im WLAN verfügbare Webseiten oder Apps können Kunden aktuelle Angebote vorgeschlagen werden.
- (66) Durch das Angebot von kostenlosen WLAN-Hotspots können Anbieter zudem – unter Beachtung der entsprechenden (auch telekommunikationsrechtlichen) Datenschutzvorschriften – Daten erheben und auswerten (dazu *Sassenberg/Mantz, WLAN und Recht, 2014, Rn. 126 ff., 141*), die bei der weiteren Verbesserung ihrer Produkte oder ihres Angebots helfen. So können über WLANs beispielsweise Kundenströme und Laufwege in Supermärkten erhoben und genutzt werden.
- (67) Die Verbreitung von kostenlosen WLAN-Hotspots hat auch positive Auswirkungen auf den (lokalen) **IT-Handel** und die Anbieter von IT-Dienstleistungen. Denn für den Aufbau müssen entsprechende Anlagen und Dienstleistungen hierfür erworben werden. Bereits seit Jahren haben sich verschiedene (teils nur lokal tätige) Unternehmen darauf spezialisiert, z.B. Hotels mit WLANs auszustatten und deren WLANs zu betreuen.
- (68) Im Übrigen erkennen mittlerweile auch **Schulen**, dass die Integration von WLAN an der Schule und im Unterricht vorteilhaft sein kann (vgl. z.B. <http://www-de.scoyo.com/eltern/aktuelles-zu-scoyo/wlan-projekt-in-hamburg>).
- (69) WLAN-Hotspots können auch der Integration dienen. So werden derzeit insbesondere auf Betreiben verschiedener lokaler Freifunk-Initiativen eine Vielzahl von **Flüchtlingsunterkünften** mit WLAN versorgt.

#### 4. SIND AUSWIRKUNGEN AUF (LOKALE) TELEKOMMUNIKATIONSBETREIBER ZU ERWARTEN, DIE INZWISCHEN VERGLEICHBARE LEISTUNGEN (Z.B. LTE) IM RAHMEN VON NUTZERVERTRÄGEN GEGEN RECHNUNG ZUR VERFÜGUNG STELLEN?

- (70) Wie oben dargestellt, geht ein Teil der Bestrebungen zum Ausbau öffentlicher WLAN-Hotspots von Telekommunikationsbetreibern aus. Für diese bieten sich beim Aufbau von WLAN-Hotspots neue Geschäftsfelder mit möglicherweise anderen/neuen Kunden. Darüber hinaus können die Betreiber positive Effekte durch die Entlastung der eigenen Netze über WLAN-Hotspots erzielen.
- (71) Bisher sind den Verfassern negative Auswirkungen insbesondere auf Mobilfunkbetreiber nicht bekannt geworden. Aufgrund der unterschiedlichen Technologie und insbesondere der sich deutlich unterscheidenden Reichweite von WLAN-Hotspots gegenüber Mobilfunknetzen findet eine Substitution von Mobilfunk aufgrund der Nutzung von WLAN bisher nicht statt. Gleiches gilt für den eigenen heimischen Internetanschluss bspw. per DSL oder Kabel.

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

(72) Praktisch alle Mobilfunkverträge mit Internetzugang enthalten derzeit eine Drosselung ab einem bestimmten pro Monat verbrauchten Datenvolumen, d.h. nach Überschreiten des vertraglich vereinbarten Datenvolumens wird die Geschwindigkeit der Datenübertragung reduziert. Für das weiter übertragene Datenvolumen fallen jedoch in der Regel keine zusätzlichen Gebühren an. Teilweise bieten Telekommunikationsbetreiber in solchen Fällen gegen Aufpreis ein weiteres Datenvolumenkontingent an. Bei einer weiteren Verbreitung von kostenlosen WLAN-Hotspots könnten weniger Nutzer diese Option nutzen. Den Verfassern liegen Erfahrungen hierzu jedoch nicht vor.

### **5. WAS IST BEIM AUFBAU EINES ÖFFENTLICH GEFÖRDERTEN UND/ODER BETRIEBENEN WLAN-NETZES IM HINBLICK AUF DAS WIRTSCHAFTSVERWALTUNGSRECHT ZU BEACHTEN, WENN BESTEHENDE WLAN-ANGEBOTE (Z.B. DURCH DIE TELEKOM) BESTEHEN?**

(73) Grundsätzlich ist Voraussetzung einer wirtschaftlichen Tätigkeit von Gemeinden, dass es sich (i.) um die Betätigung eines öffentlichen Zwecks handelt, (ii.) die Leistungsfähigkeit der Gemeinde nicht überstiegen werden darf und (iii.) die Aufgabe nicht besser bzw. ebenso gut durch Private erbracht werden kann (näher dazu *Sassenberg/Mantz, WLAN und Recht, 2014, Rn. 346 ff.*). Die ersten beiden Voraussetzungen liegen bei WLAN-Hotspots jedenfalls vor. Denn diese sind als Teil der Daseinsvorsorge anzusehen (vgl. *Haack, VerwArch 2008, 197 (205); Pünder, DVBl. 1997, 1553 (1558 f.)*). Die obigen Ausführungen belegen den öffentlichen Zweck. Darüber hinaus ist der Aufbau von WLAN-Hotspots mit relativ geringen Kosten möglich.

(74) Ob WLAN-Hotspots besser oder nicht ebenso gut von Privaten aufgebaut und betrieben werden können, wird vom konkreten Einzelfall abhängen. Den Verfassern sind keine Gerichtsverfahren oder -entscheidungen zu dieser Thematik bekannt.

(75) Im Übrigen hat sich auch die EU-Kommission im Entwurf zur Digital Single Market-Verordnung dafür ausgesprochen, dass Gemeinden öffentliche WLAN-Hotspots aufbauen und betreiben können sollten (COM (2013) 627 final, ErwGr 28):

*„Solche Einrichtungen könnten Bürgerinnen und Bürgern als Nebenleistung zu den in den betreffenden Räumlichkeiten angebotenen Diensten auch generell Zugang zu solchen Zugangspunkten gewähren; sie sollten diese Möglichkeit unter Einhaltung des Wettbewerbsrechts und der Vorschriften für die öffentliche Auftragsvergabe erhalten.“*



## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

### VI. FÖRDERPROJEKTE IM BUNDESVERGLEICH

#### 1. WELCHE STAATLICH GEFÖRDERTEN WLAN-PROJEKTE EXISTIEREN DERZEIT IN DEUTSCHLAND?

- (76) Nach Kenntnis der Verfasser gibt es mittlerweile mehrere durch staatliche Institutionen geförderte WLAN-Projekte. Insbesondere Städte, Kommunen und Länder erkennen immer mehr, dass die Förderung solcher Projekte bei geringen Kosten einen positiven Effekt hat. Die folgende Aufzählung gibt nur einen unvollständigen Ausschnitt wieder, die Links finden sich aus Gründen der Übersichtlichkeit im Anhang.
- (77) Seit dem Jahr 2012 fördert die Medienanstalt Berlin-Brandenburg (mabb) WLAN-Hotspots der Firma Kabel Deutschland. Zunächst wurden 44 Hotspots in Berlin betrieben (mabb, PM v. 19.10.2012 – [Link 1]). Mittlerweile werden in Berlin und Potsdam 100 Hotspots gefördert (mabb, PM v. 18.03.2015, [Link 2]).
- (78) Seit 2013 fördert die mabb die Berliner Freifunk-Initiative. Die mabb schreibt hierzu auf ihrer Webseite (mabb, PM v. 13.01.2015, [Link 3]):

*„Die mabb fördert damit gezielt einen Ansatz zur WLAN-Versorgung des öffentlichen Raums, der nicht-kommerziell angelegt ist und als Ergänzung bereits bestehender kommerzieller Angebote weiterentwickelt werden soll. „WLAN-Netze nehmen eine Schlüsselfunktion ein, wenn es um zeitgemäße Formen der Mediennutzung geht“, so Dr. Hans Hege, Direktor der mabb.“*

Zur Förderung der mabb und der Stadt Berlin gehört auch, dass Freifunk-Knoten auf öffentlichen Gebäuden aufgebaut werden (s. Sitzungsprotokoll des Abgeordnetenhauses Berlin v. 15.06.2015, [Link 4]).

- (79) Der Landtag Sachsen-Anhalt hat kürzlich angeregt, dass die Medienanstalt Sachsen-Anhalt ein „Pilotvorhaben im Bereich freier WLAN-Netzwerke“ starte (Beschl. v. 15.10.2015, [Link 5]).
- (80) Verschiedene Städte, Kommunen und Länder haben sich in den letzten Jahren entschieden, Freifunk-Projekte zu fördern. Die Förderung erfolgt dabei teilweise durch Bereitstellung von finanziellen Mitteln, durch Gewährung von Zugang zu kommunalen Gebäuden und Bereitstellung von Strom für dort aufgebaute WLAN-Router oder den Anschluss von WLAN- Routern an das Internet als Uplink, so z.B. in:
- Berlin-Friedrichshain [Link 6]
  - Berlin-Neukölln [Link 7]
  - Technikmuseum Berlin [Link 8]
  - Potsdam [Link 9]

## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

- Münster [Link 10]
- Gera (Pilotprojekt des Landes Thüringen [Link 11]
- Arnsberg [Link 12]
- Heidelberg [Link 13]
- Digitale Offensive Sachsen [Link 14]
- Thüringen [Link 15]
- Nordrhein-Westfalen [Link 16]
- Schleswig-Holstein [Link 17]
- Halle, Amtsblatt 18/2015 der Stadt Halle/Saale v. 14.10.2015 [Link 18]
- Linnich [Link 19]
- Aachen [Link 20]
- Dueren [Link 21]



## Stellungnahme für den hessischen Landtag „Freie WLAN-Hotspots in Hessen“

### Anhang – Linkliste staatlich geförderter WLAN-Projekte

- [1] <http://www.mabb.de/presse/pressemitteilungen/details/kabel-deutschland-und-medienanstalt-berlin-brandenburg-starten-pilotprojekt-fuer-oeffentliches-wlan-netz-in-berlin.html>
- [2] <http://www.mabb.de/presse/pressemitteilungen/details/wlan-zugang-ohne-barrieren.html>
- [3] <http://mabb.de/presse/pressemitteilungen/details/wlan-fuer-alle-freie-funknetze-in-der-praxis.html>
- [4] <http://www.parlament-berlin.de/ados/17/BuergEn/protokoll/bge17-018-ip.pdf>
- [5] <http://www.landtag.sachsen-anhalt.de/fileadmin/files/drs/wp6/drs/d4366ran.pdf>
- [6] <http://www.berlin.de/ba-friedrichshain-kreuzberg/politik-und-verwaltung/bezirksverordnetenversammlung/online/vo020.asp?VOLFDNR=5324&options=4>
- [7] <http://www.neukoellner.net/verbrauch-verzehr/neukoellner-freifunk/>
- [8] <http://netzblog.sdtb.de/ueber-den-daechern-von-berlin/>
- [9] <http://www.pnn.de/potsdam/717144/>
- [10] <https://freifunk-muensterland.de/stadt-muenster-beschliesst-unterstuetzung-von-freifunk/>
- [11] <https://www.freifunk-gera-greiz.de/web/joergd/home/-/blogs/stadt-gera-erhalt-zuschlag-fur-freifunk-forderung>
- [12] <http://www.arnsberg-info.de/arnsberg/freizeitangebote/freifunk/>
- [13] [https://www.heidelberg.de/hd,Lde/02\\_06\\_2014+Kostenloses+WLAN+in+Heidelberg.html](https://www.heidelberg.de/hd,Lde/02_06_2014+Kostenloses+WLAN+in+Heidelberg.html)
- [14] <http://www.digitale.offensive.sachsen.de/9893.html>
- [15] [http://www.mdr.de/thueringen/breitband\\_ausbau100.html](http://www.mdr.de/thueringen/breitband_ausbau100.html)
- [16] <http://www.aachener-zeitung.de/lokales/region/kostenloses-wlan-nrw-will-ausbau-foerdern-1.1122086>
- [17] <http://www.shz.de/schleswig-holstein/politik/sh-will-kostenlose-wlan-hotspots-foerdern-id9116656.html>
- [18] [www.halle.de/Publications/6293/amtsblatt18\\_141015.pdf](http://www.halle.de/Publications/6293/amtsblatt18_141015.pdf)
- [19] <http://www.aachener-zeitung.de/lokales/juelich/die-freifunk-idee-faellt-in-linnich-auf-fruchtbaren-boden-1.1084663>
- [20] [http://aachen.de/DE/stadt\\_buerger/politik\\_verwaltung/pressemitteilungen/Fluechtlingssituation.html](http://aachen.de/DE/stadt_buerger/politik_verwaltung/pressemitteilungen/Fluechtlingssituation.html)
- [21] <http://www.dueren.de/stadtinfo/freies-wlan/>