"WLAN gratis"/Public WLAN für Bayern?

Autor: Dr. K. Pfaffelmoser, Dr. M. Rothmeyer

Version: 1.0

Datum: 16.06.2015

Akosim GmbH
Sommerstr. 13
81543 München

Telefon: +49 (0)89 62439311
Telefax: +49 (0)40 25496546

Inhalt

1 Einleitung

Der Staatsminister der Finanzen, für Landesentwicklung und Heimat Dr. Markus Söder hat mit Regierungserklärung vom 27.11.2014 angekündigt, bis 2020 ein Netz für freies WLAN im ländlichen Raum zu entwickeln. In einem ersten Schritt sollen in 2015 WLAN-Hotspots an 60 Standorten bereitgestellt werden: an Digitalisierungs- und Finanzämtern, an Schlössern und Burgen sowie auf Schiffen der bayerischen Seenschifffahrt.

Die SPD-Fraktion im Bayerischen Landtag hat die vorliegende Studie in Auftrag gegeben, um Hintergrundinformationen zum Thema WLAN zu dokumentieren und um konkrete Alternativen oder Ergänzungen zu den Vorschlägen der Bayerischen Staatsregierung vorzubereiten.

2 Kurzdarstellung für Presse und Entscheider

2.1 Hintergrundinformationen

2.1.1 Technischer Hintergrund

WLAN ist in erster Linie eine Technologie, mit der ein mobiler Zugang zum Internet an Orten hergestellt werden kann, an denen bereits Internetzugang besteht. Die Qualität einer WLAN-Versorgung, gemessen an den erzielbaren Datenraten (Geschwindigkeit des Zugangs), ist dabei beschränkt auf die Datenraten des Internetzugangs, an den die WLAN-Hotspots jeweils angeschlossen sind. Mit WLAN ist es nicht oder nur in sehr begrenztem Umfang möglich, Internet- bzw. Breitbandversorgung geographisch zu auszudehnen.

WLAN-Hotspots sind entweder über einen Festnetzanschluss (DSL, VDSL) oder über einen Mobilfunkanschluss (GSM, UMTS, LTE) mit dem Internet verbunden. Um einen als störungs- bzw. verzögerungsfrei empfundenen Internetzugang für mehrere Nutzer gleichzeitig zu ermöglichen, sollte der Internetanschluss eines Hotspots idealerweise über eine Datenrate größer gleich ca. 20 Mbit/s verfügen. Ein Hotspot sollte also im Festnetz über VDSL oder im Mobilfunk mit einer der Technologien UMTS/HSPA+ oder LTE ans Internet angeschlossen sein.

Folgende Tabelle 1 gibt einen Eindruck der derzeitigen Verfügbarkeit von Breitbandanschlüssen mit einer Kapazität ≥ 16 Mbit/s in Bayern ([1]).

Kategorie	**Anteil der Haushalte**
Alle Technologien	84,9 %
Leitungsgebunden	81,9 %
Drahtlos	11,3 %
Städtisch	96,7 %
Halbstädtisch	80,4 %
Ländlich	65,1 %

Tabelle 1 Verfügbarkeit von Breitbandanschlüssen ≥ 16 Mbit/s in Bayern

In öffentlichen Verkehrsmitteln kann eine Verbindung ins Internet nur über Mobilfunk hergestellt werden. Die Abdeckung mit Mobilfunk der Technologien UMTS/HSPA und LTE ist derzeit nur in Ballungsgebieten und entlang der Hauptlinien des Bahnfernverkehrs und der Autobahnen gegeben. Prinzipiell ist eine WLAN-Versorgung in öffentlichen Verkehrsmitteln nur in diesen Gebieten möglich.

Die über WLAN abgewickelten Datenvolumina weisen über die letzten Jahre Zuwachsraten von über 80% pro Jahr auf. Es wird prognostiziert, dass solche Zuwachsraten auch in den nächsten fünf Jahren auftreten werden.

2.1.2 Rechtliche Rahmenbedingungen

In Zusammenhang mit WLAN-Versorgung ist in erster Linie die sogenannte Störerhaftung von Bedeutung. Sie hat zur Folge, dass derjenige, der einen WLAN-Zugang zum Internet bereitstellt, zunächst grundsätzlich für Schutzrechtsverletzungen (insbesondere Urheberrechtsverletzungen) auf Unterlassung in Anspruch genommen werden kann. Durch das Telemediengesetz sind Telekommunikationsbetreiber zwar für fremde Inhalte nicht verantwortlich, nach höchstrichterlicher Rechtsprechung sind Unterlassungsansprüche davon jedoch nicht erfasst. Dies gilt auch für Vereine oder Privatpersonen, die unentgeltlich einen Zugang ins Internet bereitstellen ([2]).

Das bedeutet, dass die Betreiber von öffentlich zugänglichen WLAN-Hotspots mit Abmahngebühren rechnen müssen, wenn über diesen Anschluss Urheberrechtsverletzungen erfolgen. Diese Unsicherheit ist nach Ansicht vieler Experten ein Haupthindernis für den Ausbau der öffentlichen WLAN-Versorgung in Deutschland.

Mit einem Gesetzentwurf zur Änderung des Telemediengesetzes soll für Anbieter öffentlich zugänglicher WLAN-Router Rechtssicherheit bezüglich der Störerhaftung geschaffen werden. Öffentliche WLAN-Betreiber (Kommunen, Schulen, Bibliotheken, etc.) sowie geschäftsmäßige WLAN-Betreiber (Gastronomen, Verkehrsbetriebe, Praxen, etc.) werden darin von der Störerhaftung freigestellt, wenn sie ihr WLAN durch anerkannte Verschlüsselungsverfahren (z. B. WPA2) oder vergleichbare Maßnahmen gegen unberechtigten Zugriff verschlüsseln und der Nutzer erklärt, keine Rechtsverletzung zu begehen.

Private WLAN-Betreiber sind dann von der Haftung freigestellt, wenn sie die gleichen Vorgaben erfüllen und zusätzlich den Namen der Nutzers kennen, denen sie Zugang zum WLAN ermöglichen. Protokoll- oder Dokumentationspflichten entstehen nicht.

Es ist umstritten, ob mit dem Gesetzentwurf die gewünschte Rechtssicherheit bezüglich der Störerhaftung für Betreiber von WLAN-Hotspots hergestellt wird. Ein Vergleich mit dem Ausland zeigt, dass die Rechtslage in Deutschland sehr komplex ist. So gibt es z. B. in Schweden für WLAN-Anbieter keine Störerhaftung.

Es wird empfohlen, die Störerhaftung generell auszuschließen, wenn folgende Bedingungen erfüllt sind:

- Der Nutzer bestätigt einen Hinweis auf die gesetzlichen Bestimmungen auf einer Landingpage, die auch Hinweise bezüglich der Sicherheit der Verbindung enthalten muss.
- Die MAC-ID der Nutzer wird in Logfiles festgehalten und für begrenzte Zeit gespeichert.

2.1.3 Sicherheit

Sehr viele öffentliche WLAN-Hotspots sind derzeit unverschlüsselt. Das Risiko, dass Daten abgehört werden, ist im Vergleich mit anderen Internetzugängen besonders groß, da der Funkverkehr mit wesentlich einfacheren technischen Mitteln abgehört werden kann als der Verkehr über Leitungen und Mobilfunk. Zudem ist es mit technisch einfachen Mitteln möglich einen WLAN-Hotspot vorzutäuschen. Das bedeutet, dass sich der Nutzer auf dem Hotspot des Angreifers einwählt in der Meinung, es sei der eines vertrauenswürdigen Anbieters.

Das Risiko betrifft neben dem allgemeinen Persönlichkeitsschutz insbesondere Passwörter, die bei Verbindung mit einem Internetdienst, z. B. facebook, oft automatisch und unver-

schlüsselt übermittelt werden. Der Angreifer erhält dann vollen Zugriff auf die jeweiligen Benutzerkonten des Abgehörten.

Die Sicherheit von WLAN-Hotspots kann derzeit in ausreichendem Maß durch eine der folgenden Maßnahmen sichergestellt werden:

- Es erfolgt eine individuelle Verschlüsselung jeder Verbindung vom Endgerät zum WLAN-Router mithilfe eines Authentifizierungsservers
- Es wird ein VPN-Server genutzt, mit dem der gesamte Datenverkehr zwischen VPN-Server und Endgerät (WLAN-Client) verschlüsselt wird.

2.1.4 Elektromagnetische Umweltverträglichkeit (EMVU)

Bedingt durch niedrigere Sendeleistungen und einem im Allgemeinen größeren Abstand zu den Sendeeinheiten ist die Strahlenbelastung durch WLAN deutlich geringer als die des Mobilfunks oder mobiler Telefongeräte mit DECT-Standard.

Die gesetzlich vorgeschriebenen Grenzwerte für die Strahlenimmission sind an der thermischen Wirkung elektromagnetischer Strahlen ausgerichtet. Der Verdacht, dass auch andere Schädigungseinflüsse bestehen, konnte bisher zwar nicht belegt werden, ist aber nicht gänzlich auszuschließen. Es gibt daher Empfehlungen für Grenzwerte, die um den Faktor 100 geringer sind als die gesetzlichen. Selbst diese werden von WLAN in den meisten Fällen eingehalten.

Bei größerer Verbreitung von IP-Telefonie über WLAN kann sich diese Situation ändern, da sich in diesem Fall die Sendeeinheit direkt am Kopf befindet. Es werden dann ähnliche Strahlungsbelastungen erreicht wie beim Mobilfunk.

2.1.5 Existierende Konzepte für und Implementierungen von freier WLAN-Versorgung

Die Motive und Ziele, kostenfreies öffentliches WLAN anzubieten, sind sehr unterschiedlich. In dieser Studie wird dahingehend zwischen kommerziellen, privaten nichtkommerziellen und öffentlichen (kommunalen bzw. staatlichen) Anbietern unterschieden.

Von kommerziellen Anbietern, die WLAN direkt vermarkten, wird ein zeitlich begrenzter kostenfreier Zugang als Lockangebot bereitgestellt. Andere kommerzielle Anbieter, überwiegend in der Gastronomie, bieten kostenfreies WLAN als erhöhtes bzw. zunehmend auch erwartetes Leistungsangebot.

Die Gruppe der nichtkommerziellen privaten Anbieter (Freifunk) will allgemein zugängliche Infrastruktur durch Kooperation und freiwillige Beiträge Einzelner bereitstellen. Erklärtes Ziel ist auch eine Demokratisierung der Kommunikationsmedien.

Kommunen und andere öffentliche Institutionen bieten kostenfreies WLAN an, um die Partizipationsmöglichkeiten für breite Bevölkerungskreise zu erhöhen. Weitere Motive sind die Steigerung der Attraktivität der Kommune bei Einwohnern und Gästen und die Förderung der Wirtschaft.

WLAN-Versorgung durch öffentliche Institutionen wird im Wesentlichen auf folgende Weise finanziert:

- Direkte Finanzierung aus öffentlichen Haushalten
- Finanzierung durch kommunale Versorgungsunternehmen
- Finanzierung durch Sponsoren

In deutschen Kommunen gibt es eine Vielzahl verschiedener Realisierungs- und Finanzierungsmodelle für die Bereitstellung von kostenfreien öffentlichen WLAN-Hotspots. Teils setzen Kommunen mit Fördermaßnahmen auf die Initiative privater Anbieter, teils schließen sie

sich Initiativen an und teils übernehmen sie selbst die Initiative. Mit der Implementierung werden zum Teil private Firmen beauftragt, zum Teil kommunale Versorgungsunternehmen. Bei der Finanzierung treten alle drei genannten Formen auf.

Während kostenfreies WLAN auf Flughäfen in Deutschland Standard ist und auch auf vielen größeren Bahnhöfen angeboten wird, ist das Angebot in öffentlichen Verkehrsmitteln sehr gering. Derzeit wird es nur in der 1. Klasse der ICEs, in Fernbussen und in einigen wenigen kommunalen Bussen angeboten.

Durch die Freifunk-Community werden in Deutschland 10.000 kostenfreie WLAN-Hotspots angeboten. Laut Wikipedia sind ihre „Ziele … ein hoher Grad an Zensurresistenz, eine Förderung lokaler Kommunikation, ein möglichst dezentraler Aufbau, Anonymität und Überwachungsfreiheit.“ Freifunk widmet sich auch dem Ausbau einer Vernetzung über WLAN-Richtfunk. Mit dieser Technologie wäre möglicherweise auch die geographische Erweiterung der Breitbandversorgung über WLAN möglich.

2.2 Zielsetzungen

2.2.1 Aspekte mobiler Internetnutzung

Mobiles Internet wird hauptsächlich zur Kommunikation (E-Mail, soziale Medien, WhatsApp), für kontextbezogene Informationen (Wetter, Navigation, Verkehr) und für allgemeine Suchanfragen/Recherchen verwendet. Erwartungsgemäß ist die Nutzung stark altersabhängig und nimmt mit dem Alter ab. Örtliche Abhängigkeiten der Nutzung wurden im Rahmen der Studie nicht untersucht.

Orte, an denen kostenfreie öffentliche WLAN-Versorgung bereitgestellt werden könnten, sind:

- Stark frequentierte öffentliche Plätze und Straßen
- Bahnhöfe, Haltestellen des öffentlichen (Nah-)Verkehrs
- Ämter, Behörden
- Krankenhäuser
- Alten- und Pflegeheime
- Bildungseinrichtungen und Kulturstätten: Bibliotheken, Museen, Denkmäler
- Schulen: Gymnasien, Hochschulen
- Einkaufscenter
- Freizeiteinrichtungen: Schwimmbäder, Sportstätten, Veranstaltungsorte

2.2.2 Kostenfreies WLAN im Kontext der Grundversorgung

In Deutschland besteht ein Grundversorgungsanspruch auf "Anschluss an ein öffentliches Telekommunikationsnetz und auf einen Zugang zu öffentlich zugänglichen Telefondiensten". Ein Grundversorgungsanspruch auf einen Breitband-Internetanschluss besteht jedoch nicht. In der Schweiz ist ein solcher Anspruch gesetzlich verankert, im Rahmen der EU wird seine Einführung diskutiert.

Nur wenige Grundversorgungsleistungen sind kostenfrei (z. B. Straßen und Bildung). Die meisten müssen in Abhängigkeit von den bezogenen Leistungen bezahlt werden. Bei einem Grundversorgungsanspruch auf Breitbandanschluss steht die Kostenpflichtigkeit nicht zur Debatte. Vor diesem Hintergrund ist ein Grundversorgungsanspruch auf kostenfreies WLAN nicht gerechtfertigt.

Versorgungsziele kommunaler und staatlicher Stellen sind

1. die Bereitstellung allgemein zugänglicher Infrastruktur, um möglichst breiten Bevölkerungskreisen Teilhabe zu ermöglichen
2. Erhöhung der Attraktivität der Kommune bzw. der Region
3. Förderung der Wirtschaft

Aufgrund der in Abschnitt 2.1.5 dargestellten Interessenslagen ist für Zielsetzung 1 ein ausreichender Gestaltungsspielraum erforderlich. Dieser ist nur gewährleistet, wenn sich die Kommune oder staatliche Stelle, die eine kostenfreie öffentliche WLAN-Versorgung bereitstellen will, ausreichend finanziell beteiligt.

2.3 Umsetzungskonzepte

Im Folgenden werden Umsetzungskonzepte vorgeschlagen für die Förderung von kostenfreiem öffentlichen WLAN

- im öffentlichen Raum
- in Bildungseinrichtungen und Kulturstätten
- in öffentlichen Verkehrsmitteln
- durch nichtkommerzielle, private Initiativen (Freifunk)

Die Konzepte beinhalten größtenteils auch Kostenkalkulationen. Da die Eingangsgrößen nicht zuverlässig abgeschätzt werden können, bieten die Kalkulationen nur grobe Abschätzungen und geben lediglich Größenordnungen der zu erwartenden Kosten wieder.

2.3.1 Freie WLAN-Versorgung im öffentlichen Raum

Zur Förderung von kostenfreiem öffentlichen WLAN im öffentlichen Raum werden folgende Maßnahmen vorgeschlagen:

Zur Förderung kommunaler WLAN-Versorgung:

- Finanzielle Zuschüsse an Kommunen bei der Einrichtung einer WLAN-Versorgung
- Rahmenverträge mit Anbietern von Internetanschlüssen, Hard- und Softwareanbieter und Installationsfirmen zugunsten der Kommunen und anderer zuständiger staatlicher Stellen
- Logistische Unterstützung durch ein Zentrum des Landes (z. B. IT-Dienstleistungszentrum des Freistaats Bayern) bezüglich Installationsberatung, Bereitstellung von Hard- und Firmware, Sicherheits-Infrastruktur (Authentifizierungsserver, VPN-Server etc.)

Zur Förderung der Wirtschaft:

- Bereitstellung einer Infrastruktur für geschäftsmäßige WLAN-Betreiber, die kostenfreies öffentliches WLAN bereitstellen, z. B. Hardware, Firmware und Sicherheitsinfrastruktur (Authentifizierungsserver, VPN-Server etc.)

Bei der Kalkulation der Kosten wird zwischen WLAN-Hotspots in Gebäuden und im Freien unterschieden. Bei einem Versorgungsgrad von 200 Hotspots pro 1 Mio. Einwohner in Gebäuden und 500 Hotspots pro 1 Mio. Einwohner im Freien (das wären für München ca. 280 Hotspots in Gebäuden und 700 Hotspots im Freien) werden die jährlichen Gesamtkosten auf ca. 7,8 Mio. EUR geschätzt.

Bei einem Versorgungsgrad von 300 Hotspots pro 1 Mio. Einwohner in Gebäuden und 800 Hotspots pro 1 Mio. Einwohner im Freien (das wären für München ca. 420 Hotspots in Gebäuden und 1120 Hotspots im Freien) würden sich die jährlichen Gesamtkosten auf ca. 16,6 Mio. EUR belaufen.

2.3.2 Förderung von freiem WLAN in Bildungseinrichtungen und Kulturstätten

Für Bildungseinrichtungen und Kulturstätten werden die gleichen Maßnahmen vorgeschlagen wie für die Versorgung im öffentlichen Raum.

Die Versorgung an Hochschulen erscheint bereits ausreichend und wird in Kostenkalkulationen nicht berücksichtigt.

Bei der Versorgung von Schulen werden drei Modelle kalkuliert. Bei ca. 4500 Schulen mit ca. 55.000 Klassen in Bayern ergeben sich folgende jährliche Gesamtkosten

Modell	**Kosten**
WLAN in Lehrerzimmern	2,49 Mio. EUR
WLAN in Lehrerzimmern und speziellen Computerlehrräumen (bei einem Computerlehrraum pro 10 Klassen)	5,52 Mio. EUR
WLAN in Lehrerzimmern und allen Klassenzimmern	32,87 Mio. EUR

Tabelle 2 Kosten für WLAN in Schulen

Die jährlichen Kosten für die Ausstattung der 1153 bayerischen Museen mit WLAN würden sich auf ca. 1,9 Mio EUR belaufen. Dabei wurde ein Bedarf von ca. 3 Hotspots pro Museum unterstellt.

2.3.3 Förderung von freiem WLAN im öffentlichen Personennahverkehr

Der öffentliche Personennahverkehr (ÖPNV) gliedert sich in den Schienenpersonennahverkehr (SPNV) und in kommunal organisierten Personennahverkehr.

Die Bereitstellung von WLAN im SPNV ist grundsätzlich nur in Gebieten möglich, in denen eine ausreichende Mobilfunkversorgung mit den Systemen UMTS/HSPA oder LTE gegeben ist. Dies trifft nur auf Ballungsräume und ihr näheres Umfeld zu. Da die Kosten für die Nachrüstung von Fahrzeugen des SPNV mit WLAN erheblich höher sind als der geplante Einbau in Neufahrzeugen, ist damit zu rechnen, dass WLAN erst in Neufahrzeugen bereitgestellt wird. Aus diesen Gründen kann der Beginn der Einführung von WLAN im SPNV in frühestens fünf Jahren erwartet werden.

Die Kosten müssten von den Aufgabenträgern des SPNV getragen werden, die ihrerseits über den Bundeshaushalt finanziert werden. Die Aufgabeträger beklagen, dass die Mittel derzeit nicht ausreichend sind, den SPNV in seinem derzeitigen Umfang aufrecht zu erhalten. Werden die Mittel im Bundeshaushalt nicht wesentlich erhöht, muss damit gerechnet werden, dass eine Finanzierung von WLAN zugunsten dringenderer Aufgaben zurückgestellt werden muss.

Realistische Kostenschätzungen sind aufgrund fehlender Informationen über den Einbau von WLAN in den Fahrzeugen nicht möglich. Dennoch wurde beispielhaft eine Kalkulation für die WLAN-Versorgung im Münchner Verkehrsverbund durchgeführt unter der fiktiven Annahme, dass die Installation pro Fahrzeug 25.000 EUR kostet und die Amortisationszeit bei 10 Jahren liegt. Dabei ergäben sich jährliche Kosten in Höhe von ca. 5,6 Mio. EUR.

WLAN in Verkehrsmitteln des kommunal organisierten ÖPNV (überwiegend Busverkehr) kann durch Bezuschussung von WLAN-Implementierungen gefördert werden.

2.3.4 Förderung einer privaten, nichtkommerziellen freien WLAN-Versorgung bzw. Vernetzung

Der Freifunk kann durch eine gezielte Öffentlichkeitsarbeit bezüglich der Freifunk-Konzepte und durch Bereitstellung von best practice Beispielen in Zusammenarbeit mit Freifunk-Gruppen und Open Source Vereinen gefördert werden.

3 Hintergrundinformationen

3.1 Allgemeines

Das Thema „Freies WLAN“ ist ein Unterthema des Themas „Freier Zugang zum Internet über Funk“ bzw. ein Unterthema des noch umfassenderen Themas „Freier Zugang zum Internet“. Aufgrund der physikalischen Grundlagen für die Übertragung von Informationen über Funk ergibt sich, dass für die Übertragung einer bestimmten Menge von Informationen in einem bestimmten geographischen Gebiet ein bestimmter, minimaler Frequenzbereich des elektromagnetischen Spektrums genutzt werden muss. Die für Informationsübertragung nutzbaren Frequenzen (150 kHz bis 70 GHz) sind limitiert. Durch die Internationale Behörde für Standardisierung von Funkfrequenzen (ITU) wird sichergestellt, dass der verfügbare Frequenzraum möglichst effizient und standardisiert genutzt wird.

Heute und auf für die nächsten 10 Jahre ist absehbar, dass die zur Verfügung stehenden Frequenzen für Mobilfunk (GSM, UMTS, LTE) bereits sehr stark ausgelastet sind und auch nicht wesentlich ausgedehnt werden können (weil diese Prozesse alleine mehrere Jahre an Arbeit von Experten in den internationalen Standardisierungsgremien erfordern).

Die einzige kurzfristige und für die nächsten Jahre verfügbare Alternative zur Übertragung per Funk bietet für die WLAN-Technik (im englischen Sprachraum ist der Begriff „WiFi“ gebräuchlich).

Die Übertragung von Daten über Funk durch und für private und geschäftliche Nutzer von und zum Internet wird daher in den nächsten Jahren in erheblichem Maß von der Art und Weise abhängen, wie schnell und intensiv WLAN genutzt werden kann.

Die derzeit zugeteilten WLAN Frequenzen erlauben die Übertragung sehr großer Datenmengen (derzeit bis zu 3,5 GBit/s), bei Verwendung einer sehr kostengünstigen Technik.

Neben der Breitbandförderung betreffend DSL, VDSL u.a. Festnetzanschlüsse ist daher die Förderung bzw. der Aufbau von freiem WLAN-Zugang zum Internet eine aussichtsreiche Möglichkeit, den freien Zugang zum Internet für große Nutzerzahlen zu ermöglichen.

Die WLAN-Technik unterscheidet sich von Mobilfunk im Wesentlichen durch folgende Charakteristika:

- WLAN-Technik ist Low-Cost-Technik und damit etwa einen Faktor 100 bis 1000 kostengünstiger als Mobilfunk. (WLAN-Router gibt es von 20 bis 300 Euro, Mobilfunkbasistationen kosten 30.000 bis 500.000 Euro.)
- WLAN wurde primär optimiert für lokale Nutzer, d.h. Nutzer, die sich nur in der engeren Umgebung einer Basisstation (WLAN-Router) bewegen.
- Wegen der niedrigen Einstiegsschwelle gibt es eine sehr große Anzahl kommerzieller und auch gemeinnütziger Betreiber von WLAN-Inseln und auch WLAN-Insel-Verbundnetzen.
- Die legale Nutzung von WLAN-Technik umfasst auch den Aufbau von Low-Cost-Richtfunkstrecken. Derartige Richtfunkstrecken sind nicht genehmigungspflichtig und können prinzipiell zum Aufbau von WLAN-Insel-Verbundnetzen oder zur WLAN-Anbindung ans Internet genutzt werden. Die Kosten für derartige Richtfunkstrecken liegen im Bereich zwischen 100 Euro und 2000 Euro.
- WLAN-Sende-Empfangs-Geräte (Router) sind bei Einhaltung der genormten Leistungsgrenzen genehmigungsfrei und nicht meldepflichtig (im Gegensatz zu Mobilfunk-Basistationen).
- Die Reichweite von WLAN-Basistationen liegt im Bereich von 100 bis 200 Metern, während Mobilfunkbasistationen bis zu 25 km Reichweite haben können.

Aufgrund der vorgenannten Charakteristika ist es grundsätzlich möglich, mit WLAN-Technik Funknetze aufzubauen, die zu einem gewissen Grad Mobilfunknetze ergänzen, teils auch ersetzen können. Man kann also verstehen, warum die Nutzung von WLAN in den letzten Jahren so stark um sich gegriffen hat.

Den Vorteilen und dem Potential von WLAN-Technik stehen aber auch einige gravierende Nachteile gegenüber:

- WLAN-Netze sind nicht geeignet um mobile Teilnehmer mit einer zuverlässigen Telefonverbindung zu versorgen.
- Die Standardisierung von größeren WLAN-Insel-Verbundnetzen ist weitgehend eine Standardisierung innerhalb eines Firmenstandards. Internationale, herstellerübergreifende Standards sind nicht etabliert.
- die Sicherheit in WLAN-Netzen ist zweifelhaft oder nur unter engen Voraussetzungen gegeben, siehe Abschnitt 3.4.
- der Aufbau von Funkzellen für größere Nutzerzahlen ist limitiert auf einen Radius von ca. 200 Metern. Darüber hinaus kann WLAN nur mit Spezialantennen gebündelt gesendet und empfangen werden.

Aus den oben genannten Charakteristika folgt, dass sich WLAN global betrachtet überwiegend für folgende Anwendungsszenarien eignet:

- Nutzung in Ergänzung von Mobilfunknetzen überall dort, wo Nutzer hohe Datenraten benötigen und sich nicht gleichzeitig über Distanzen von mehr als 100 Metern bewegen.
- Versorgung von Hallen, Gebäuden-und Sportstätten.
- Versorgung von Nutzern in Wohnungen für den Transfer von hohen Datenraten.

Mit Rücksicht auf die vorgenannten Randbedingungen kann man folgende visionäre Ziele definieren:

- WLAN sollte kurzfristig maximal genutzt werden um den kostengünstigen Zugang zum Internet zu beschleunigen und zu verbessern.
- existierende WLAN-Standards sollten weiter fortgeschrieben werden um die Lücken zu stopfen (IT-Security, Meshed-Netze)
- Vereine und Organisationen, die WLAN-Netze betreiben und fördern, sollten seitens des Staates unterstützt werden, mit dem Ziel, sinnvolle Standards für alle Nutzer zu unterstützen.
- Die Entwicklung von Standards, WLAN-Technik und Software für WLAN-Nutzung sollte kurzfristig gefördert werden.
- Um die stärkere Verbreitung von WLAN zu fördern, sollte auf die Störerhaftung komplett verzichtet werden (s. Abschnitt 3.3).

3.2 Technischer Hintergrund

WLAN ist in erster Linie eine Technologie, mit der ein mobiler Zugang zum Internet an Orten hergestellt werden kann, an denen bereits Internetzugang besteht. Die Qualität einer WLAN-Versorgung, gemessen an den erzielbaren Datenraten, ist dabei beschränkt auf die Datenraten des Internetzugangs, an den die WLAN-Hotspots jeweils angeschlossen sind. Mit WLAN ist es nicht oder nur in sehr begrenztem Umfang möglich, Internet- bzw. Breitbandversorgung geographisch zu auszudehnen.

Die technischen Hintergründe für diese Aussagen werden im Folgenden dargestellt. Vor dem Hintergrund typischer Internetanwendungen und der für sie erforderlichen Datenraten wird

ein Überblick gegeben über die Technologien und die mit ihnen einhergehenden Datenraten von derzeit gebräuchlichen Internetzugängen.

Ein rasanter technischer Fortschritt auf allen im Folgenden dargestellten Gebieten und die immense Diversifizierung der technischen Möglichkeiten machen eine exakte Darstellung im Rahmen dieser Untersuchung unmöglich. Daher werden jeweils Werte oder Wertebereiche angegeben, die den derzeit überwiegend verwendeten oder allgemeingültig spezifizierten Stand der Technik widerspiegeln. Aktuell erreichte Spitzen- oder Rekordwerte in einzelnen Technologien sind nicht berücksichtigt. Oftmals weichen die tatsächlich in der Praxis erreichten Leistungen von den theoretisch möglichen ab. Dies ist, soweit möglich, dargestellt.

3.2.1 Datenraten

Für den Internetzugang stehen verschiedene Technologien zur Verfügung. Ein wesentliches Kriterium der Technologien ist die Geschwindigkeit des Zugangs, die dem Anwender damit zur Verfügung steht. Diese wird messbar in Form von Datenraten.

Um die Auswirkungen unterschiedlicher Datenraten einschätzen zu können, wird im Folgenden ein Überblick über erforderliche Datenraten verschiedener Internetanwendungen gegeben. Dabei wird unterschieden zwischen Echtzeit-Anwendungen (im Wesentlichen Audio- und Video-Streaming), bei denen eine Mindestdatenrate erforderlich ist, um eine zufriedenstellende Funktion zu gewährleisten, und Nicht-Echtzeit-Anwendungen, bei denen kürzere oder längere Wartezeiten die wesentlichen Funktionen nicht beeinträchtigen aber als störend empfunden werden können.

In folgender Tabelle 3 sind Datenraten für Audio- und Video-Streaming dargestellt. Insbesondere bei Video-Streaming gibt es eine immense Anzahl von Konfigurationsmöglichkeiten bezüglich Auflösung und Komprimierungsverfahren ([3], [4]). Davon ist eine kleine Auswahl beispielhaft dargestellt. Da die erforderlichen Datenraten von den Videoinhalten abhängen (je mehr Bewegung, desto höher die Datenrate), ist jeweils ein Bereich angegeben.

Nutzungsart	**Typische Datenrate**
Skype ([5])	
Audio	0,1 Mbit/s
Video	0,3 Mbit/s
Video (High-Quality)	0,5 Mbit/s
Video (HD)	1,5 Mbit/s
Audio	
starke Qualitätseinbußen	ca. 8 – 96 kbit/s
leichte Qualitätseinbußen	ca. 0,1 – 0,32 Mbit/s
kaum wahrnehmbare oder keine Qualitätseinbußen	ca. 0,32 Mbit/s – 5 Mbit/s
Video	
640 x 360 Pixel (YouTube)	0,4 – 1,0 Mbit/s
640 x 480 Pixel (VGA/SD)	1,0 – 1,7 Mbit/s
800 x 480 Pixel (WVGA)	1,2 – 2,1 Mbit/s
1280 x 720 Pixel (HD720)	2,0 – 5,0 Mbit/s

Tabelle 3 Datenraten von Echtzeit-Anwendungen

In folgender Tabelle 4 sind die typischen Datenvolumina von Internet-Anwendungen und die Datenraten gelistet, die erforderlich sind, um eine Wartezeit von 1 Sekunde zu ermöglichen ([6], [7], [8]).

Nutzungsart	Datenvolumen	Datenrate bei 1 sec Wartezeit
E-Mail ohne Anhang	< 10 kB	> 0,08 Mbit/s
E-Mail mit Anhang	ca. 0,1 – 5 MB	0,8 – 40,0 Mbit/s
Internet-Seite z. B. Google Maps	0,1 – 1 MB 0,1 MB	0,8 – 8,0 Mbit/s 0,8 Mbit/s

Tabelle 4 Datenvolumina von Nicht-Echtzeit-Anwendungen

Der Anschluss an das Internet kann über Kabel (Kupfer- oder Koaxialkabel, Glasfaserkabel) oder über Funk hergestellt werden. Für die Datenübertragung werden jeweils verschiedene Systeme eingesetzt, wobei bei der Kabelanbindung DSL/VDSL derzeit vorherrschend ist. Im Mobilfunk gibt es die Technologie-Generationen G2 (GSM), G3 (UMTS mit HSPA und HSPA+) und G4 (LTE, LTE –A).

In Tabelle 5 und Tabelle 6 sind die wesentlichen technischen Systeme für den Internetzugang mit ihren Datenraten aufgeführt ([9], [10], [11]). Bei den Funksystemen ist jeweils die typische bzw. die maximale Reichweite mit angegeben.

System	Maximale Datenrate Downlink (Uplink)
DSL (Kabel)	8-24 (1) Mbit/s
VDSL (Kabel)	25-200 (5-40) Mbit/s
Glasfaser	200/300 Mbit/s

Tabelle 5 Datenraten leitungsgebundener Systeme

System	Max. Brutto-Datenrate Downlink (Uplink)	~ Netto-Datenraten Downlink (Uplink)	Reichweiten typisch / maximal
Mobilfunk ([12])			1 – 5 km / 20 km
EDGE (GSM)	236,8 kbit/s	<< - <[1] 236,8 kbit/s	
UMTS	384 kbit/s	<< - < 384 kbit/s	
HSPA	7,2 (5,8) Mbit/s	<< - < 7,2 (5,8) Mbit/s	
HSPA+	42,2 (11,5) Mbit/s	<< - < 42,2 (11,5) Mbit/s	
LTE	100 (50) Mbit/s	<< - < 100 (50) Mbit/s	
LTE –A	1000 (500) Mbit/s	<< - < 1000 (500) Mbit/s	
WLAN ([13])			100 m / 300 m im Freien 20 – 40 m in Gebäuden 1 – 5 km mit Richtfunkantenne
IEEE 802.11a, g, h	54 Mbit/s	20 – 22 Mbits/s	
IEEE 802.11n	150/300/450 Mbit/s	--/120/170 Mbit/s	
IEEE 802.11ac	1300/2600/6900 Gbit/s	660/--/3500 Mbit/s	
WiMAX ([14])	15/75 Mbit/s	1 – 6 Mbit/s	1,5 – 5 km / 50 km
Richtfunk[2] ([15], [16])	2–1000 Mbit/s	2–1000 Mbit/s	2 – 30 km / 90 km

Tabelle 6 Datenraten von Funksystemen

[1] << - <: wesentlich kleiner bis kleiner

[2] Richtfunk ist hier aufgeführt, da er oft für die Anbindung von Mobilfunkzellen an das Festnetz genutzt wird und damit einen Einfluss auf Datenraten haben kann (s. auch Abschnitt 3.2.2)

Beim Mobilfunk sind die Netto-Datenraten kleiner oder erheblich kleiner als die Brutto-Datenraten, da sie sehr stark von der Entfernung zur Funkzelle abhängen. Unter sehr günstigen Bedingungen können jedoch die Brutto-Datenraten annähernd erreicht werden ([17], [18]).

Im Gegensatz zum Mobilfunkt enthält die Brutto-Datenrate bei WLAN auch den durch Kodierung und Fehlerkorrekturverfahren bedingten Overhead. Die Netto-Datenrate ist daher in jedem Fall wesentlich geringer als die Brutto-Datenrate.

Der Vollständigkeit halber ist der Standard WiMAX hier mit aufgeführt. Die angegebenen Datenraten wurden in der Praxis nicht erreicht. WiMAX spielt für die Internetversorgung in Deutschland praktisch keine Rolle mehr.

In Verkehrsmitteln wie z. B. in Fernzügen, oder –bussen oder auf Schiffen der Binnenschifffahrt, sind WLAN-Hotspots über Mobilfunk an das Festnetz angeschlossen. I. d. R. ist die Kapazität der WLAN-Verbindung dann durch die Kapazität des Mobilfunkkanals beschränkt. Einen Überblick über die theoretisch maximal möglichen Nutzerzahlen bei Echtzeitanwendungen gibt folgende Tabelle 7. In der Praxis liegen die Werte für die Mobilfunkanwendungen bei 50 – 80% der angegebenen Werte.

Internetzugänge über Mobilfunk und über WLAN werden von mehreren Nutzern gleichzeitig verwendet. Da bei einer WLAN-Anbindung über Mobilfunk nur ein Anwender die Mobilfunkverbindung verwendet (der WLAN-Hotspot oder das WLAN-Netz), sind Beschränkungen der Nutzerzahlen pro Zelle in der Tabelle nicht berücksichtigt. Bei WLAN hängen Beschränkungen der Zahl der Nutzer vom verwendeten Gerät ab. Auch hier sind diese Beschränkungen in der Tabelle nicht berücksichtigt. Realistisch sind maximale Werte im zweistelligen bis niedrigen dreistelligen Bereich. Um völlig unrealistische Werte zu vermeiden, sind in der Tabelle die Werte auf 256 beschränkt. Eine theoretische Überschreitung dieses Werts ist durch gelbe Hinterlegung (256) gekennzeichnet.

Nutzungsart	UMTS	HSPA	HSPA+	LTE	LTE –A	WLAN 11a,g,h	WLAN 11n	WLAN 11ac
Max. Nutzer	4	15	15	--	--	--	--	--
Skype								
Audio	3	72	422	1.000	10.000	220	256	256
Video	1	24	140	333	3.333	73	256	256
Video (High-Quality)	-	14	84	200	2.000	44	256	256
Video (HD)	-	4	28	66	666	14	113	256
Audio								
starke Qualitätseinbußen	48	75	5275	12.500	125.000	220	256	256
leichte Qualitätseinbußen	3	22	422	1.000	10.000	68	256	256
geringe Qualitätseinb.	1	1	131	312	3.125	4	256	256
Video								
640 x 360 Pixel (YouTube)	-	15	15	250	2.500	22	256	256
640 x 480 Pixel (VGA/SD)	-	7	105	100	1.000	12	256	256
800 x 480 Pixel (WVGA)	-	6	42	83	833	10	170	256
1280 x 720 Pixel (HD720)	-	3	35	50	500	4	85	256

Tabelle 7 Anzahl gleichzeitiger Nutzer von Echtzeit-Anwendungen

3.2.2 WLAN Anbindungen

Da die Reichweite eines WLAN-Routers maximal 300 m beträgt, ist eine WLAN-Versorgung im Wesentlichen auf geographische Bereiche beschränkt, in denen bereits eine Breitbandversorgung existiert. Die Kapazität von WLAN-Routern ist wesentlich durch die Anbindungsmöglichkeiten an das Breitbandnetz bestimmt.

In der folgenden Abbildung 1 sind die wesentlichen Anbindungsmöglichkeiten von öffentlichen WLAN-Routern an das Breitbandnetz schematisch dargestellt.

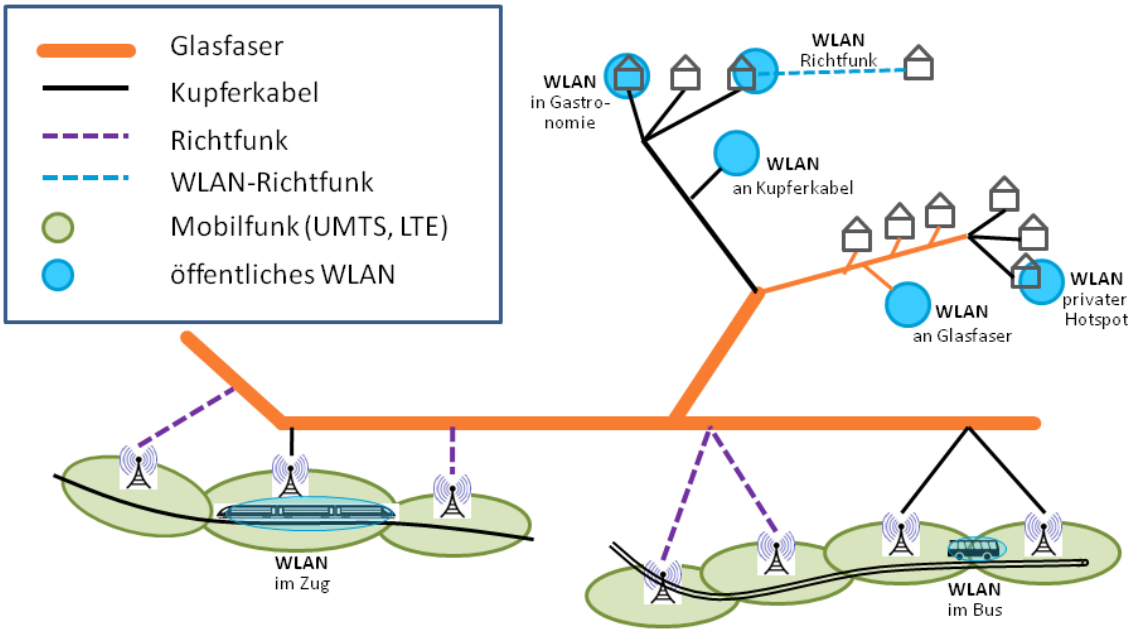

Abbildung 1 WLAN Anbindungen an das Festnetz (wesentliche technische Möglichkeiten)

Das Rückgrat (Backbone) der Datenübermittlung im Internet bilden Glasfaserverbindungen, die eine sehr hohe (praktisch unbegrenzte) Übertragungskapazität bereitstellen. Aufgrund der steigenden Anforderungen an die Datenraten beim Endnutzer wird der Ausbau von Glasfasernetzen stark vorangetrieben. Insbesondere in Ballungsgebieten werden Glasfaseranschlüsse zu den Häusern verlegt und können auch im Haus bis hin zu den angeschlossenen Geräten eingerichtet werden ([19]).

Der weitaus größte Teil der stationären Anschlüsse ist jedoch nach wie vor über Kupferkabel angebunden. Aus Tabelle 5 ist in Zusammenhang mit Tabelle 3 ersichtlich, dass auch über Kupferkabel relativ hohe und für die meisten Anwendungen bei weitem ausreichende Datenraten erzielt werden.

In Abbildung 1 sind die wesentlichen Möglichkeiten dargestellt, öffentliche WLAN-Hotspots mit dem Internet zu verbinden:

- direkte Verbindung zum Glasfasernetz:
  z. B. öffentliche WLAN-Hotspots in Norderstedt und München
- direkte Verbindung zum Kupferkabelnetz:
  z. B. öffentliche WLAN-Hotspots von Kabel Deutschland
- Verbindung über einen häuslichen Festnetzanschluss (Kupfer oder Glasfaser):
  z. B. WLAN-Hotspots in der Gastronomie, z. T. Hotspots der Freifunk-Community
- Verbindung über Mobilfunk:
  z. B. WLAN-Hotspots in ICEs und Fernbussen und in der Bayerischen Seenschifffahrt

Aus Abbildung 1 werden auch die eingangs von Abschnitt 3.2 gemachten Aussagen ersichtlich, nämlich dass

- mit WLAN in erster Linie ein mobiler Zugang zum Internet an Orten hergestellt werden kann, an denen bereits Internetzugang besteht.

- die Qualität einer WLAN-Versorgung, gemessen an den erzielbaren Datenraten, auf die Datenraten des Internetzugangs beschränkt ist, an den die WLAN-Hotspots jeweils angeschlossen sind.
- es mit WLAN nicht oder nur in sehr begrenztem Umfang möglich ist, Internet- bzw. Breitbandversorgung geographisch zu auszudehnen.

Eine weitere Anbindungsmöglichkeit, die derzeit vor allem von der Freifunk-Community genutzt wird, ist WLAN-Richtfunk. Dabei werden Daten zwischen zwei Standorten (Point-to-Point) im WLAN-Standard mit Richtantennen übertragen, womit die Reichweite auf bis zu 5 km (und mehr) erhöht werden kann ([20], [21]). Mit dieser Technik wäre auch eine geographische Ausdehnung der Internetversorgung grundsätzlich möglich, sie wird derzeit jedoch nicht für eine breite Anwendung genutzt.

3.2.3 Frequenzspektrum

Derzeit bestehen für WLAN-Funkanwendungen in Deutschland Allgemeinzuteilungen in folgende Frequenzbereichen ([22], [23]):

Frequenzbereich [MHz]	Zuteil.-Art	Max. Strahlungsleistung (EIRP)	Örtliche Einschränkungen
2400,0 – 2483,5	Sekundär[3]	0,1 W Summenleistung[4]	Keine
5150,0 – 5350,0	Sekundär	0,2 W mittlere Leistung, 0,01 W/MHz	Nur in geschlossenen Räumen
5470,0 – 5725,0	Sekundär	1 W mittlere Leistung, 0,03 W/MHz	Keine

Tabelle 8 Datenraten verschiedener Internetnutzungsarten

Insgesamt stehen damit 538,5 MHz Spektrum für WLAN zur Verfügung. Für den Mobilfunk (GSM, UMTS, LTE) steht in Deutschland derzeit ein Spektrum von 625 MHz zur Verfügung. Die Zuteilung für den Mobilfunk ist primär, d. h. der Mobilfunk darf durch sekundäre Funkdienste nicht gestört werden. Im Gegensatz zu WLAN kann damit das zugeteilte Spektrum von Mobilfunkanwendungen uneingeschränkt genutzt werden.

Es gibt Empfehlungen an die Europäische Kommission, das WLAN-Funkanwendungen zugeteilte Frequenzspektrum auf 5150 MHz bis 5925 MHz auszuweiten und weltweit für WLAN verfügbar zu machen ([24]).

3.2.4 WLAN-Nutzung und Offloading

Mit Offloading wird die Nutzung ergänzender Technologien für die Datenübermittlung im Mobilfunk bezeichnet. Im Vergleich mit WLAN ist die Datenübertragung mit Mobilfunk sehr teuer. Dies gilt insbesondere für die Versorgung in Gebäuden. Die Datenraten von WLAN sind in der Tendenz eher höher als die des Mobilfunks (s Tabelle 6). Da zudem die Versorgungsflächen von WLAN-Routern i. d. R. wesentlich kleiner sind, als die von Mobilfunkzellen, kann über WLAN wesentlich mehr Datenverkehr pro Fläche und Frequenzspektrum abgewickelt werden als über Mobilfunk. Daher entlastet WLAN insbesondere in Ballungsgebieten zunehmend das Mobilfunknetz.

Dies wird u. a. in einer Studie des WIK gezeigt, in der die in Deutschland pro Monat übertragenen Datenvolumina im Mobilfunk und die WLAN-Offload-Volumina im Zeitraum 2011 bis 2016 ermittelt bzw. geschätzt wurden ([24], S. 110). Die Werte sind in folgender Tabelle 9 und Abbildung 1 dargestellt.

[3] Sekundäre Funkdienste dürfen primäre nicht stören, genießen selbst aber keinen Schutz gegenüber anderen Funkdiensten

[4] Der Wert beschränkt die Summe der Sendeleistung(en) über den gesamten Frequenzbereich

	2011	2012	2013	2014	2015	2016	Ø Zuwachs pro Jahr
Mobilfunk	7,5	13,5	24,3	42,5	72,5	118,6	73,7%
WLAN	31,7	62,4	122,9	226,8	400,4	673,6	84,3%

Tabelle 9 Monatliche Datenvolumina Mobilfunk, WLAN-Offload in PByte/Monat

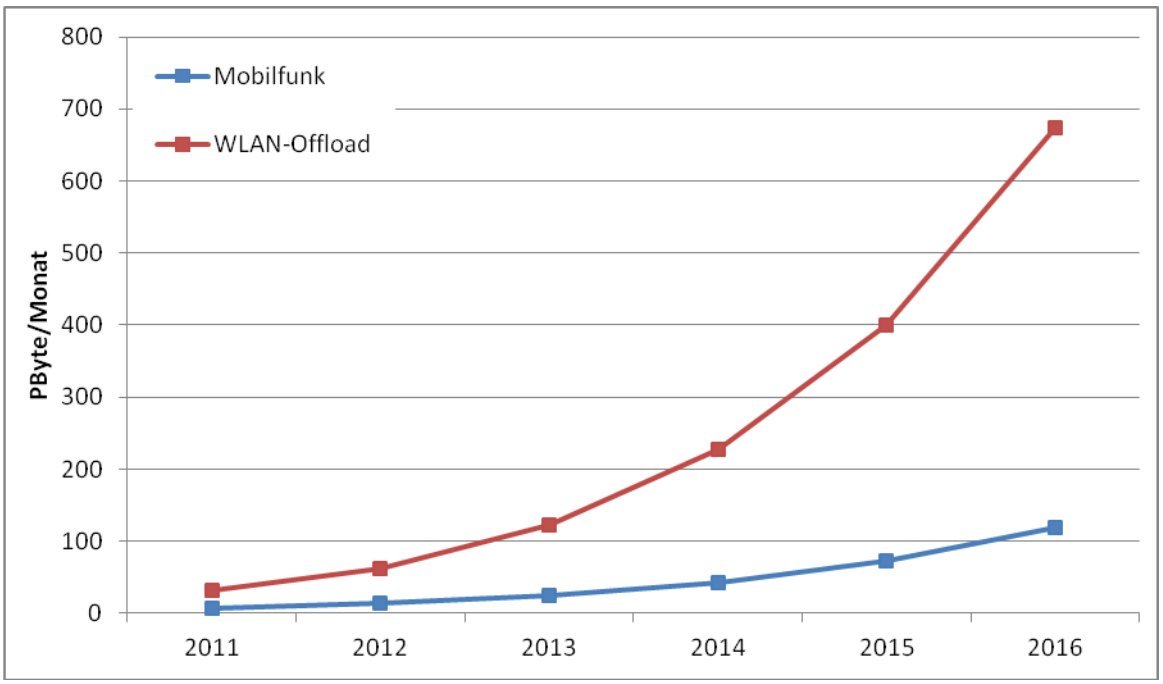

Abbildung 2 Monatliche Datenvolumina Mobilfunk, WLAN-Offload

Offload durch Smartphones, Mobiltelefone und Tablets wird hauptsächlich an privaten WLAN-Routern genutzt. An öffentlichen WLAN-Routern ist das erforderliche Login eine Hemmschwelle. Der im Rahmen der Wi-Fi Alliance zertifizierte Standard Passpoint™ und der WLAN-Standard 802.11u ermöglichen inzwischen eine automatische Einwahl und Authentifizierung für Geräte mit SIM-Karte (s. [24], S. 33).

3.3 Rechtliche Rahmenbedingungen

Die rechtlichen Rahmenbedingungen für den Betrieb von WLAN-Netzen gehen aus dem Telemediengesetz hervor. Die derzeitige Rechtslage beinhaltet eine grundsätzliche Unterscheidung zwischen Telekommunikationsbetreibern und sonstigen Betreibern.

Während in der jetzigen Rechtslage und Rechtsprechung die Telekommunikationsbetreiber von einer Haftung weitgehend freigestellt werden, gelten für private Anbieter oder auch für kommerzielle Anbieter, die nicht als Telekommunikationsanbieter gelten, sehr umfangreiche Vorschriften, welche darauf hinauslaufen, dass ein erhebliches Haftungsrisiko für die Gruppe der Nicht-Telekommunikationsanbieter besteht.

Für Nicht-Juristen sind diese Rechtsvorschriften schwer nachvollziehbar.

Ein Blick auf die europäische Ebene zeigt, dass die rechtlichen Rahmenbedingungen europaweit sehr unterschiedlich definiert sind. Auf der einen Seite gibt es Länder wie z.B. Schweden, in denen die Störerhaftung praktisch komplett entfällt. Das andere Extrem ist in diesem Fall die Rechtslage Deutschland, wo die Störerhaftung gesetzlich und durch Gerichtsurteile sehr kompliziert geregelt ist.

Im Folgenden wird zunächst auf die derzeitige gesetzliche Regelung in der Bundesrepublik eingegangen, dann auf die in Diskussion befindliche Neuregelung (der sogenannte „Referentenentwurf“ der Regierungsparteien in Berlin).

Zuletzt wird in Abschnitt 3.3.3 ein Vergleich auf europäischer Ebene gezogen und in Abschnitt 3.3.4 aus der Sicht der Autoren beschrieben, welche Art der gesetzlichen Regelung aus der Sicht der WLAN-Anwender zu einem bestmöglichen Erfolg führen würde.

3.3.1 Aktuelle Rechtslage in Deutschland

Die aktuelle Rechtslage ist für Telekommunikationsbetreiber im Wesentlichen in Paragraph 8 des Telemediengesetzes festgelegt (siehe Anhang 1 und [25])

Die Rechtslage für alle übrigen Anbieter von WLAN-Netzen ergibt sich aus dem Urheberrecht, dem Markenrecht, dem Wettbewerbsrecht, dem Persönlichkeitsrecht und einer größeren Zahl diesbezüglicher Gerichtsurteile auf verschiedenen Ebenen bis zum Bundesgerichtshof (BGH) (siehe auch „Ansprüche geschädigter Dritter“, ([26], S. 209ff).

Die aktuelle Rechtslage stellt die Telekommunikationsanbieter im Wesentlichen von Ansprüchen der Inhaber von Urheber-, Marken- und Wettbewerbsrechten frei. Der Telekommunikationsbetreiber muss im Zweifelsfall auf Gerichtsbeschluss hin offenlegen, wer zu einem bestimmten Zeitpunkt eine bestimmte Internetadresse für Datenübertragung benutzt hat. Bei Nachweis von Rechteverletzungen haftet der Anbieter jedoch nicht für Schadenersatz. Auch eine strafrechtliche Haftung z.B. bei der Verbreitung illegaler Inhalte entfällt, sofern dem Anbieter nicht nachgewiesen werden kann, dass er mit dem Nutzer zusammenarbeitet oder von den illegalen Inhalten Kenntnis hatte.

Im Gegensatz dazu führt die aktuelle Rechtsprechung dazu, dass private Anbieter von WLAN-Netzen und auch geschäftliche Anbieter, die nicht Telekommunikationsbetreiber im engeren Sinn sind, mit hohen Kosten bedroht werden:

- Abmahnkosten, eingefordert zum Beispiel von Anwaltskanzleien, die sich auf die Abmahnung von Rechteverletzungen im Internet spezialisiert haben.
- Schadenersatzforderungen der Inhaber von Urheber- und Markenrechten, oder von Unternehmen, die einen Verstoß gegen das Wettbewerbsrecht einklagen.

3.3.2 Geplante Änderungen

Der vorliegende Entwurf vom 11.23.2015, „Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG)“ sieht folgende wesentliche Änderungen vor:

1. Öffentliche WLAN-Betreiber (Kommunen, Schulen, Bibliotheken, etc.) sowie geschäftsmäßige WLAN-Betreiber (Gastronomen und Cafés, Verkehrsbetriebe, Praxen, etc.) genießen eine Haftungsfreistellung, wenn sie ihr WLAN durch anerkannte Verschlüsselungsverfahren (z. B. WPA2) oder vergleichbare Maßnahmen gegen den unberechtigten Zugriff verschlüsseln und der Nutzer erklärt, keine Rechtsverletzung zu begehen.
2. Private WLAN-Betreiber sind dann von der Haftung freigestellt, wenn sie die gleichen Vorgaben erfüllen und zusätzlich den Namen des Nutzers kennen, welchem sie Zugang zum WLAN ermöglichen. Protokoll- oder Dokumentationspflichten entstehen nicht.
3. Schließlich soll mit dem Gesetzentwurf klargestellt werden, dass das Haftungsprivileg der Hostprovider gem. § 10 TMG (Internet-Service-Provider, die fremde Inhalte für Dritte speichern) dann nicht gelten soll, wenn ihr Geschäftsmodell im Wesentlichen auf der Verletzung von Urheberrechten beruht.

Auf den ersten Blick hört sich dies nach einer klaren und für öffentliche und private wie geschäftliche WLAN-Betreiber günstigen Regelung an.

Nach Veröffentlichung dieses sogenannten „Referentenentwurfes“ wurde im Internet in verschiedensten Veröffentlichungen eine große Zahl von Einwänden erhoben. Es sollen hier nur einige wesentliche Einwände aufgeführt werden. So wird der Entwurf als „schwammig“ eingeschätzt, zu erkennen an folgenden Beispielen:

- was heißt „anerkannte Verschlüsselungsverfahren“ oder „vergleichbare Maßnahmen“ konkret?
- was heißt es, den Namen des Nutzers zu kennen? Laut Personalausweis, laut mündlicher Auskunft des Nutzers, laut Eingaben in einem Formular, weil der Nutzer persönlich bekannt ist?
- unter welchen Umständen beruht ein Geschäftsmodell „im wesentlichen“ auf Rechteverletzungen? Wenn die Mehrzahl der Cafe-Besucher nur ins Cafe kommt, um über Internetverbindung auf ausländischen Servern Nazi-Literatur durchzulesen, die in Deutschland auf dem Index stehen?

Weitere umfangreiche Kritik an diesem Entwurf findet man z.B. auf folgenden Internetseiten:

- https://netzpolitik.org/2015/bundesregierung-schuetzt-abmahnindustrie-keine-abschaffung-der-stoererhaftung-fuer-buerger/
- https://www.datenschutzbeauftragter-info.de/kritik-referentenentwurf-zur-stoererhaftung-bei-wlan/
- http://www.internet-law.de/2015/03/verschlimmbesserung-der-gesetzesentwurf-zur-stoererhaftung-von-w-lan-betreibern.html
- http://www.golem.de/specials/stoererhaftung/

Konkrete Kritikpunkte aus den Diskussionen im Internet:

- Der Zwang zur Kenntnis der Namen der Nutzer widerspricht dem Datenschutz.
- Die Verpflichtung zur Nutzung von Verschlüsselung erfordert ein Management bzw. eine Verteilung der WLAN-Passworte, was erheblichen Aufwand generieren kann.
- WLAN-Verschlüsselung ist ohnehin nicht 100% sicher, sollte daher über offenes WLAN plus selbst gewähltes VPN genutzt werden.
- Nutzer werden Phantasienamen nutzen, daher bewirkt die Verpflichtung zur Kenntnis des Nutzernamens nichts.

3.3.3 Vergleich Rechtslage WLAN mit dem Ausland

Ein umfangreicher Vergleich der deutschen Rechtslage in Sachen WLAN mit dem Ausland ist nicht Gegenstand der Studie. Es soll hier lediglich Top-Down betrachtet werden, wie die Gesamtwirtschaft durch eine Freigabe von WLAN beeinflusst wird.

In manchen Ländern wird die WLAN-Nutzung praktisch gar nicht rechtlich reglementiert, so zum Beispiel in Schweden und in manchen Staaten der USA. Hinweise auf die Situation in Schweden sind sehr zahlreich im Internet zu finden.

Einige Hotspotbetreiber in Deutschland speisen den an einem deutschen Hotspot gesammelten WLAN-Verkehr in Schweden ins Internet ein („Peering in Schweden“) um die Störerhaftung in Deutschland zu umgehen ([27], [28], [29]).

Es gibt nach Kenntnis der Autoren keine allgemein bekannten negativen Auswirkungen in Schweden oder USA auf die Gesamtsituation von Rechteinhabern dergestalt, dass ein großer Schaden entsteht durch die Freigabe der WLAN-Nutzung.

Im nächsten Abschnitt wird deshalb die weitgehende Freigabe von WLAN auch in Deutschland vorgeschlagen.

3.3.4 Optimierung der Rahmenbedingungen für WLAN-Nutzung

Volkswirtschaftlich betrachtet ist der Einfluss von Mobilfunk und WLAN auf die Gemeinkosten viel größer als der Öffentlichkeit bewusst ist. In einem Paper der Europäischen Union wird abgeschätzt, dass bei optimaler Nutzung von WLAN der Einspareffekt gegenüber einem Ausbau von ausschließlich Mobilfunk (Technologien 3G/4G/5G) bis 2016 kumulativ im Bereich von 300 Milliarden Euro (für das Gebiet der EU) liegt ([24], S. 5).

Allerdings basiert diese Abschätzung auf der Annahme, dass WLAN technisch und organisatorisch viel enger mit der Mobilfunktechnik gekoppelt wird, als es in dem vorliegenden Paper angenommen wird. Eine entsprechende Diskussion der engen Integration von WLAN und Mobilfunk wurde aus dem vorliegenden Paper ausgeklammert, weil dies den Rahmen der Studie sprengen würde.

Die Größenordnung des oben genannten Einspareffektes macht es sinnvoll, im Sinn einer Top-Down-Betrachtung eine Optimierung der rechtlichen Bedingungen für die Nutzung von WLAN zu fordern. Eine Optimierung der technisch-organisatorischen Gegebenheiten ist auf Basis geänderter rechtlicher Bedingungen dann erheblich leichter.

Aus Sicht der Autoren sind folgende rechtliche Voraussetzungen für eine optimale Nutzung von WLAN erforderlich:

- In der Gesetzgebung der BRD wird die Störerhaftung auf ein notwendiges Minimum reduziert. Die Betreiber der Free-WLAN-Hotspots müssen dann keine Kosten durch Rechtsstreitigkeiten mehr fürchten, wenn sie vorgegebene (leicht erfüllbare) Auflagen erfüllten, wie z. B.:
  - Einbau einer Landingpage mit
    - Hinweis auf die gesetzlichen Bestimmungen bezüglich WLAN-Nutzung auf einer Landingpage.
    - Hinweis auf die Notwendigkeit zur Nutzung von VPN um einen Missbrauch der Daten zu verhindern.
  - das Führen von Logfiles
    - mit Aufzeichnung der MAC-ID des Nutzers.
    - mit ausreichende Sicherheit gegen das Hacken der Logfiles.
- die BRD erlässt eindeutige Bestimmungen, die eine Klage der Netzbetreiber gegen die kommerzielle (bzw. „freie“) Nutzung eines privaten DSL-Anschlusses verhindern. Derzeit ist dieser Punkt noch nicht erfüllt, da eine Klage von 1&1 zwar bis zum Bundesgerichtshof eskaliert wurde, jedoch dann durch eine außergerichtliche Einigung beigelegt wurde und daher höchstinstanzlich noch nicht entschieden ist ([30], [31]).

Alternativ sind auch noch weniger restriktive Varianten denkbar (Wegfall der Landingpage). Allerdings bietet eine Vorschrift für eine Landingpage mehrere Vorteile:

1. Für alle Nutzer werden die in Deutschland geltenden rechtlichen Bestimmungen explizit genannt. Insbesondere für ausländische Nutzer ist dies wichtig, da deutsches Recht in Bezug auf Datensicherheit und Schutz privater Daten erheblich von manchen ausländischen Rechtsordnungen abweicht.
2. die Landingpage bietet die Möglichkeit zur Platzierung von Werbung und erlaubt es damit, einen Teil der Kosten der WLAN-Infrastuktur zu refinanzieren.

3.4 Sicherheit

Während im Bereich Mobilfunk von Anfang an eine strenge Normierung der Technik – inklusive der Sicherheitsstandards – durchgesetzt wurde, ist dies leider bei WLAN nicht der Fall.

Im Bereich WLAN gibt es eine Anzahl verschiedener Techniken und Standards. Die Beurteilung der Sicherheit von WLAN-Netzen ist nicht einfach. Es werden hier nur die besten 2 Methoden zur Herstellung akzeptabler Sicherheit in WLAN-Netzen behandelt:

1. WPA2-verschlüsseltes WLAN
2. Offenes WLAN in Kombination mit VPN-Tunnel, der die Daten der Nutzer gegen Manipulation und Ausspähen schützt.

3.4.1 Warum ist die Sicherheit im WLAN so wichtig?

Viele Nutzer besitzen zuhause oder im Büro einen Festnetzzugang zum Internet und wickeln über diesen all ihre kritischen Aktionen ab, wie zum Beispiel:

- Internet Banking
- Internet Shopping, mit
    - Kreditkarteninformationen
    - Bankkonto-Informationen
- Austausch von (unverschlüsselten) Mails mit vertraulichem Inhalt.

Allerdings bürgert es sich immer mehr ein, Tablet PC, Smartphone oder auch Laptop unterwegs für manche dieser Aktionen zu nutzen.

Für den Nutzer ist dabei oft nicht klar erkennbar, welche Informationen durch den Browser verschlüsselt (z.B. über https) mit dem Internet ausgetauscht werden und welche nicht. Dies liegt daran, dass potentiell jedes Tab-Pane, jedes Fenster des Browsers, ja sogar jeder Popup-Dialog einen Wechsel der Kommunikationsmethode von https (verschlüsselt) zu http (unverschlüsselt) bedeuten kann.

Bei Nutzung eines WLAN ist prinzipbedingt der gesamte Verkehr für den Inhaber des Routers sichtbar. D.h. die Daten, die über den WLAN-Router laufen können archiviert und an ganz anderer Stelle ausgewertet werden, z.B. wenn ein Mafioso einen Router in einem Restaurant betreibt.

Es besteht daher bei Nutzung eines WLAN immer die Gefahr, dass Daten, die über einen fremden Router laufen, missbraucht oder weiterverkauft werden. Im sogenannten „Darknet“ gibt es einen schwunghaften Handel mit derartigen Daten. Der bekannteste illegale Markt war „Silk Road“ (siehe https://de.wikipedia.org/wiki/Darknet-Markt).

In Abschnitt 3.4.4.5 schildern wir zur Verdeutlichung der Gefahren von ungesichertem WLAN-Betrieb, wie jemand mit minimalem Aufwand mit einem mobilen Gerät eine Abhöraktion durchführen kann.

3.4.2 Vergleich Sicherheit Festnetz zu WLAN

Wer einen Festnetzanschluss nutzt, ist im Wesentlichen abhängig von folgenden Faktoren (Beispiel hier: DSL-Zugang):

- Es kann jemand die Telefonleitung anzapfen (im Verteilerkasten im Keller eines Wohnhauses, im Verteilerkasten auf der Straße, in der Vermittlungsstelle des Netzbetreibers, in den höheren Netzzentren.
- Zum Abhören ist physikalischer Zugriff nötig.
- Die entsprechenden Orte sind normalerweise versperrt, und nur ein bestimmter Personenkreis hat Zugang (Mitbewohner in einer Wohngemeinschaft, Hausmeister, Personal des Netzbetreibers, externes Personal, welches vom Netzbetreiber beauftragt wurde).

Im Gegensatz dazu kann bei Nutzung eines WLAN potentiell jeder, der sich in einem Umkreis von bis zu 200 Meter befindet eine Attacke per Funk durchführen:

- ohne Schlüssel
- ohne weitere Kenntnis, auf Basis von Software, die per Download im Internet verfügbar ist
- mit geringsten Kosten (normaler Laptop mit WLAN-Interface)

3.4.3 Überblick WLAN Sicherheit

WLANs werden nahezu überall verwendet. Die WLAN Sicherheit hängt sehr stark von dem verwendeten Standard ab. Hier wird in sehr kurzer Form zusammengefasst, wie man die Sicherheit im WLAN-Bereich optimieren kann.

Ergebnis von Internetrecherchen, Gesprächen mit Experten und eigenen Erfahrungen:

- Es gibt nur einen Standard, nämlich WPA2, der auf einfachem Weg eine halbwegs sichere Kommunikation über WLAN ermöglicht.
- Auch WPA2 hat konzeptionelle Lücken, die von Crackern genutzt werden können.
- Um in WLAN-Netzen einen verbesserten Schutz vor Crackern zu erreichen, muss WPA2 durch eine Methode zur Verwaltung der Passworte ergänzt werden, so dass je Nutzer ein separates Passwort verwendet wird.
- Wenn kein VPN aufgebaut werden kann, dann muss die Nutzung der WLAN-Verbindung (bei offenen und auch bei verschlüsselten WLANs) auf die Nutzung des Browsers via HTTPS beschränkt bleiben, ansonsten ist die Sicherheit der Daten nicht gegeben.

Fazit:

1. WLAN ist auf Basis derzeit verfügbarer Standards, wie z.B. WPA2-Verschlüsselung, kein wirklich sicheres Kommunikationsmedium.
2. Wenn die Datensicherheit gewährleistet werden soll, muss WLAN deshalb immer in Kombination mit einem VPN-Tunnel genutzt werden.
3. Wer WLAN-Hotspots ohne VPN verwendet, muss sich über sämtliche im Hintergrund ablaufenden Kommunikationsverbindungen des Betriebssystems und aller darauf laufenden Prozesse im Klaren sein.

   Konkret: jegliche Übermittlung von Passworten und sonstigen vertraulichen Informationen muss durch geeignete Einstellung einer lokalen Firewall verhindert werden.

3.4.4 IT-Security-Problemstellungen in WLAN-Netzen

3.4.4.1 Auswahl der Verschlüsselungsmethode

Die Beschreibungen im Internet sind so verklausuliert, dass viele Nutzer nicht erkennen, dass WPA2 der einzig sinnvolle Standard für Verschlüsselung ist.

3.4.4.2 Kompatibilität

Aufgrund eigener Erfahrung sind viele WLAN-Endgeräte bei Verwendung von WPA2 mit einer erheblichen Zahl von WLAN-Routern nicht kompatibel. Dem Nutzer bleibt dann nichts anderes übrig, als einen „unsicheren“ Verschlüsselungsstandard zu verwenden. Oft ist dies dann aus Frust über verlorene Zeit der „offene“ Modus, also gar keine Verschlüsselung.

3.4.4.3 Performance ist abhängig von der Verschlüsselung

Wer sich die Mühe macht, die Geschwindigkeit der Datenübertragung auf WLAN mit verschiedenen Verschlüsselungsmethoden zu vergleichen, wird bei manchen Endgeräte-Router-Kombinationen eine starke Abhängigkeit der Performance feststellen.

Aus eigener Erfahrung: speziell Jugendliche ändern dann den Verschlüsselungsmodus im Home-WLAN auf „offen“, damit zum Beispiel ein Fußballspiel in voller Auflösung über Internetverbindung angesehen werden kann. Die Eltern bekommen dies oft gar nicht mit.

Oft bleibt es dann bei der unsicheren Einstellung, zumindest für gewisse Zeit.

3.4.4.4 Reichweite ist abhängig von der Verschlüsselung

Neben der Performance ist (bei manchen Kombinationen von WLAN-Endgerät und Router) auch die Reichweite des WLAN von der Verschlüsselungsmethode abhängig. Dies liegt daran, dass beim Aufbau der Verbindung bei Verwendung von z.B. WPA2 erheblich mehr Daten ausgetauscht werden müssen als ohne Verschlüsselung. Dadurch kann es zu Time-Out-Problemen kommen, wenn man in größerer Entfernung vom Router eine Verbindung aufbauen will, z.B. aus einem anderen Stockwerk.

3.4.4.5 Problem der Entscheidung für ein WLAN

WLAN ist nahezu überall verfügbar. Eine Beurteilung der Vertrauenswürdigkeit der Anbieter ist allerdings sehr schwierig. Ein normaler Nutzer kann vor dem Aufbau einer WLAN Verbindung nämlich nur anhand des Netz-Namens (SSID) und anhand der angezeigten Verschlüsselungsart (WPA, WPA2, WEP,...) beurteilen, wie vertrauenswürdig ein WLAN-Netz ist. Dies ist jedoch trügerisch, wie das folgende Beispiel zeigt:

Manager *Heinzelmann* sitzt in einem großen Vortragssaal einer Konferenz. Er sieht sich einen Vortrag über IT-Security an. In den Vortragsunterlagen findet er die Info; „unser Hotspot für Gäste steht ihnen mit der Kennung „WLAN_Saal1“ zur Verfügung, das Passwort lautet „2015_04_03_667489123“. Manager *Heinzelmann* startet also seinen Laptop, öffnet dann den Dialog für die Auswahl von WLAN-Netzen und wählt das Netz „WLAN_Saal1“ mit Verschlüsselung WPA2 aus, er gibt hier das o.g. Passwort ein, die Verbindung wird erfolgreich aufgebaut.

Was der Manager nicht bemerkt hat, ist, dass es zwei WLAN-Netze mit gleicher SSID, also gleichem Netznamen gibt:

- das offizielle WLAN-Netz des Veranstalters, „WLAN_Saal1“ mit WPA2-Verschlüsselung
- ein Netz mit gleichem Namen, auch genannt „WLAN_Saal1“, auch mit WPA2-Verschlüsselung. Dieses Netz ist allerdings kein Netz des Veranstalters, sondern ein Netz, welches von einem mobilen Gerät aus aufgebaut wurde, vom Laptop des Privatdetektivs *Spürhund*, der eine Sitzreihe hinter dem Manager sitzt

Da der Name eines WLAN-Netzes nicht geschützt werden kann, können beliebige Nutzer unter beliebigen Namen WLAN-Netze betreiben. Bei der Anzeige der WLAN-Netze (für Netze, die den gleichen Namen tragen) im Auswahldialog für die Netze (SSIDs) gilt:

- Der Netzwerkname erscheint nur einmal

Nach Auswahl des Netzes durch den Nutzer wird dann - ohne dass der Nutzer darüber informiert wird -automatisch das Netz mit der höheren Feldstärke am Ort des Nutzers aktiviert.

Konsequenz: da *Spürhund* sehr nahe bei *Heinzelmann* sitzt, ist die Feldstärke des betrügerischen WLANs am Ort von *Heinzelmann* größer als die des Konferenz-WLAN. *Heinzelmann* wählt daher, ohne es zu wollen, das von *Spürhund* aufgebaute betrügerische WLAN aus.

Da der Aufwand zum Betrieb eines betrügerischen WLAN-Netzes minimal ist, besteht praktisch keine finanzielle Hürde für Cracker.

Fazit: WPA2 ist keine Lösung, die ausreichend Schutz bietet.

Die einzige bekannte einfache und dennoch sichere Lösung (nach derzeitigem Kenntnisstand) wird nachfolgend beschrieben.

3.4.5 Sichere WLAN-Nutzung durch Verwendung eines VPN

Eine sichere Nutzung unverschlüsselter WLAN-Netze kann durch Verwendung eines VPN-Tunnels erreicht werden. Das VPN wird vom mobilen Endgerät bis zu einem vertrauenswürdigen VPN-Server im Internet aufgebaut.

Konkret ist bei IT-Security-Experten folgende Methode zur sicheren Nutzung von WLAN-Datenübertragung gebräuchlich:

Nutzung von offenen Hotspots, ohne Verschlüsselung, mit:

1. Aufbau der Verbindung ohne Verschlüsselung
2. Auswahl eines sicheren VPN-Servers im Internet
3. Aufbau eines VPN-Tunnels zwischen dem Mobilen Endgerät und dem VPN-Server
4. Nutzung der VPN-Verbindung, der Datenverkehr ist von außen nicht mehr entschlüsselbar

Diese Vorgehensweise kann bei professioneller Konfiguration des mobilen Endgerätes und Konfiguration von geeigneten VPN-Servern automatisch erfolgen, zum Beispiel in dem Moment, in dem eine Treibersoftware feststellt, dass kein Festnetzanschluss und keine Mobilfunk-Netzverbindung verfügbar sind, jedoch Empfang eines offenen WLAN möglich ist.

3.4.6 Überblick über technische Standards

Ein Überblick über die Verschlüsselungs- und Authentifizierungsmethoden im Bereich WLAN ist hier verfügbar:
https://de.wikipedia.org/wiki/Wireless_Local_Area_Network#Datensicherheit

Wegen der (auch im Rahmen von BSI-Papers) bekannt gewordenen Probleme mit den meisten WLAN-Verschlüsselungs-Standards konzentriert sich die Diskussion der WLAN-Sicherheit im Rahmen dieses Kapitels auf die Verschlüsselung WPA2 oder auf offene WLAN-Netze in Kombination mit einem VPN.

3.4.7 Empfehlungen

Das Bundesamt für Sicherheit in der Informationstechnik hat Hinweise zum sicheren Betrieb von WLANs herausgegeben BSI: WLAN Sicherheitstipps. Nachfolgend werden Empfehlungen gegeben, in denen die Empfehlungen des BIS berücksichtigt und konkretisiert werden.

Der einzige Verschlüsselungsstandard, der für WLAN überhaupt unter gewissen Bedingungen akzeptable Sicherheit bietet, ist WPA2/Enterprise. In der Folge diskutieren wir daher nur diesen Standard und VPN-Lösungen.

Es ist bekannt, dass in einem WPA2-verschlüsselten WLAN-Netz ein Nutzer, der das Passwort kennt, alle anderen mit relative begrenztem Aufwand abhören kann (s. http://www.heise.de/security/meldung/Sicherheitsluecke-in-WPA2-entdeckt-1044869.html).

3.4.7.1 Empfehlungen an die Nutzer von WLAN-Netzen mit WPA2-Verschlüsselung

Die Sicherheit eines WPA2-verschlüsselten WLAN-Netzes hängt davon ab, wer das Passwort kennt. Sehr stark ist dies abhängig von folgenden Punkten: der Gruppe von Personen, der Zugriff gestattet wird, der Art der Passwortverwaltung, der Frequenz des Passwortwechsels, der Länge der Passworte, der Art, wie diese erzeugt werden.

Es wird empfohlen für die Verwaltung, Verteilung und Wahl der Passworte:

- Passworte helfen nur, wenn diese geheim gehalten werden.

- Essentiell ist die Auswahl der Personen, die sie als „vertrauenswürdig“ einstufen und denen ein Passwort mitgeteilt wird. Dies gilt insbesondere, wenn kein RADIUS-Server zur Verwaltung einzelner Passworte verwendet wird.
- Konzepte, bei denen eine große Zahl von Mitarbeitern das gleiche Passwort für einen WLAN-Hotspot oder eine ganze Gruppe von Hotspots nutzen, sind daher von vorne herein untauglich für die Herstellung der IT-Sicherheit.
- Wenn Passworte über unverschlüsselte e-Mails durch Internet geschickt werden, dann gefährdet dies die IT-Sicherheit. Die Passwort-Verteilung muss also über einen sicheren Kanal erfolgen.
- Um eine Geheimhaltung der Passworte sicherzustellen, sollte WPA2 plus ein RADIUS-Server (vorzugsweise jedoch ein Diameter-Server) betrieben werden. Pro Nutzer wird dann ein separates Passwort generiert und verwaltet.
- Passworte im WLAN sollten mit einem Zufallsgenerator erzeugt werden und die laut WPA2-Standard maximale Länge (63 Buchstaben) haben.
- Da nicht ausgeschlossen werden kann, dass ein Passwort in falsche Hände gerät, ist die Verwendung von MAC-ID-Filtern sinnvoll, die nur bestimmte Geräte in Kombination mit bestimmten Passworten zulassen. Vorbildlich ist in dieser Hinsicht die von Google propagierte 2-Faktor-Authentisierung (s. https://www.google.com/landing/2step/).
- Leider führen MAC-ID-Filter und auch zwangsweiser Wechsel von Passworten immer zu erhöhtem Aufwand, entweder auf Seiten der Nutzer oder bei den Administratoren, oder beiden.
- Um hohe Sicherheit zu erreichen, wäre ein periodischer zwangsweiser Wechsel des Passwortes an und für sich sinnvoll, zum Beispiel einmal im Monat. Realistisch ist dies aber nicht, weil hierdurch zu viel manueller Aufwand und damit Zeitverlust beim Nutzer entstehen würde, d.h. dies wäre keine praxisnahe Empfehlung.

3.4.8 Anmerkungen zu speziellen WLAN-Features

3.4.8.1 Unterdrückung der SSID

Die Unterdrückung des WLAN-Netznamens (der SSID) bringt keine zusätzliche Sicherheit, verursacht jedoch in vielen Fällen Störungen bei der Kommunikation, da nicht alle WLAN-Endgeräte mit dieser Option einwandfrei funktionieren.

3.4.8.2 Nutzung von MAC-ID-Filtern

Die Nutzung eines MAC-Filters (Media Access Control, s. http://de.wikipedia.org/wiki/MAC-Adresse) zur Ablehnung unbekannter Geräte in einem WLAN-Netz bietet zusätzlichen Schutz, da unbekannte Geräte abgelehnt werden können, selbst wenn diese das korrekte Passwort verwenden. Die MAC-ID-Filterung schützt allerdings nicht vor Profi-Crackern. Inzwischen bieten manche Betriebssystem sogar die Möglichkeit die MAC-ID der Netzwerkkarte per Software zu ändern, (für Windows 7 s. http://www.tecchannel.de/netzwerk/tipps/2032725/mac_adresse_von_installierten_adaptern_unter_windows_aendern/)

3.4.8.3 Nutzung von RADIUS-Server für die Authentifizierung mit Einzelpasswort pro Nutzer

Um die Möglichkeit zu erschweren, dass sich ein Cracker das WLAN-Passwort des Routers besorgt, ist die Verwendung von separaten Passwörtern pro Nutzer ein probates Mittel. Hierfür werden häufig sogenannte „RADIUS-Server“ eingesetzt. Seit dem Jahr 2000 ist allerdings bekannt, dass RADIUS-Server auf einem Standard beruhen, der methodisch fragwürdig und damit unsicher ist (s. http://www.untruth.org/~josh/security/radius/radius-auth.html). RADIUS

ist somit nicht zu empfehlen, sondern der Nachfolgestandard „Diameter“, der jedoch nur von wenigen Herstellern unterstützt wird.

3.4.9 Empfehlung für WLAN Einzelnutzer

Sofern ein einziger Nutzer per WLAN-Router angebunden werden soll, kann WPA2 mit relativ hoher Sicherheit genutzt werden. Allerdings muss ein langes Passwort (63 Buchstaben, zufallsgeneriert) verwendet werden, welches keinem anderen Nutzer bekannt sein darf.

3.4.10 Alternativen zu WLAN

Wer kein VPN über WLAN nutzen möchte oder kann, aber auf Sicherheit Wert legt, sollte auf WLAN komplett verzichten und über Mobilfunk mit dem Internet Verbindung aufnehmen. Achtung: die Sicherheit der Verbindung hängt vom Standard (GSM, UMTS, LTE) und natürlich der Professionalität des Netzbetreibers ab. Leider ist die Sicherheit in Mobilfunknetzen ohne VPN deshalb eher eine Unsicherheit.

3.4.11 Nutzeraufklärung

Eine umfassende Aufklärung der Nutzer von WLAN-Zugriffspunkten ist essentiell. Dabei muss insbesondere auf die automatischen und freiwilligen Sicherheitsvorkehrungen sowie auf die geltende Gesetzeslage aufmerksam gemacht werden.

Normalerweise sind folgende Methoden für die Nutzeraufklärung gebräuchlich:

- Login-Dialog

  Hier erfolgt die Aufklärung nicht per Dialog ad hoc, sondern in dem Moment, wenn der Nutzer die Vertragsbedingungen für die Nutzung des Login akzeptiert.
- Landingpage

  Um dem neu angemeldeten WLAN-Nutzer diese Nutzeraufklärung zu vermitteln, muss eine sogenannte „Landingpage“ eingerichtet werden. Sie entspricht in etwa dem Konzept eines Webproxys und leitet die erste Anfrage des Browsers auf eine Webseite weiter, die zur Kenntnisnahme der oben genannten Hinweise auffordert. Erst dann wird dem neuen Nutzer Zugriff auf das Internet gewährt.
- Konzept der Selbstverantwortung

  Das radikalste Konzept basiert auf komplett offenen Hotspots (also unverschlüsselt, keine Hindernisse, kein Login, keine Landing Page). Die Aufklärung der Nutzer muss in diesem Fall allerdings auf einem anderen Kanal erfolgen:
  - bei Restaurants z.B. in der Speisekarte
  - in Unternehmen z.B. durch Aushang für die Mitarbeiter und Besucher

  Bei der jetzigen Gesetzeslage in Deutschland ist ein derartiges Konzept wegen der Störerhaftung nicht machbar.

  Im Rahmen dieses Konzeptes sind die Nutzer komplett selbstverantwortlich, müssen sich also zum Beispiel durch Verwendung eines VPN-Tunnels, den sie in eigener Verantwortung aufbauen, schützen. Das Konzept hindert den Nutzer nicht an einer Nutzung des Internetzugangs, bei der die Daten des Nutzers von beliebiger Seite ausgespäht werden können.

  Im Rahmen des Konzeptes können dennoch Zeitlimits für die Nutzung und/oder Bandbreitenbeschränkungen für die Nutzer gelten.

3.4.12 Sicherheit durch VPN

Eine echte Sicherheit für Hotspots, die mehrere Nutzer unterstützen sollen, ist derzeit nach Kenntnisstand der Autoren nur mit VPN machbar. Durch Nutzung des VPN-Kanals ist es dann sogar möglich, offene Hotspots zu verwenden, was die Performance erhöht und viele

Störungen vermeidet, die in der Praxis in WLANs mit WPA2 auftreten (z.B. durch inkompatible Implementierungen der Verschlüsselung bzw. der Treiber verschiedener Geräte).

3.4.13 Warum nicht das Firmen-VPN verwenden?

Viele Nutzer lösen die Sicherheitsprobleme im Zusammenhang mit WLAN-Nutzung dadurch, dass sie sich eine Erlaubnis des Arbeitgebers für Heimarbeit geben lassen. Bei guter Begründung wird dies aus betrieblichen Gründen (Vorteile für das Unternehmen) heute bei vielen Unternehmen genehmigt.

Das Unternehmen stellt dem Mitarbeiter dann einen VPN-Zugang zur Verfügung, in Form von:

- VPN-Client, also einer Software zum Zugang ins Internet per VPN.
- einen VPN-Server, d.h. einen Hostnamen, mit Portnummer, Login und Passwort, manchmal zusätzlich mit Hardware-Sicherung in Form von USB-Stick, Zugangskarte, etc.

Der Mitarbeiter kann dann - je nach Konfiguration der Firewall-Regeln im Unternehmen - unter Umständen auch aus dem Ausland über VPN ins Firmennetz und von dort zu facebook, Google, Twitter und allen anderen Internetadressen.

Potentiell gefährdet der Mitarbeiter durch Nutzung eines offenen Hotspots die Sicherheit des Unternehmensnetzes, wenn dieses nicht professionell aufgebaut bzw. gepflegt ist. Die Gefahr entsteht dadurch, dass ein Angreifer auf dem Endgerät des Nutzers die entschlüsselten Daten abgreifen kann, nachdem zum Beispiel er einen sogenannten „Keylogger“ installiert hat.

Eine Trennung von privatem WLAN-Zugang und VPN-Firmenzugang über WLAN ist daher unbedingt angesagt. Deshalb wird hier die Nutzung eines eigenen (privaten) VPN-Zugangs für jeden Nutzer empfohlen.

3.5 Elektromagnetische Umweltverträglichkeit (EMVU)

Schädigungen der menschlichen Gesundheit durch elektromagnetische Strahlung können verschiedene Ursachen haben. In den für WLAN relevanten Frequenzbereichen 2,4 GHz und 5 GHz können bisher – wissenschaftlich eindeutig – nur Schädigungen aufgrund von Wärmeentwicklung im biologischen Gewebe nachgewiesen werden. Die Wärmeentwicklung hängt dabei wesentlich von der physikalischen Größe „Leistungsflussdichte“ des elektromagnetischen Feldes ab, dem das Gewebe durch WLAN-Geräte ausgesetzt ist ([32], S 32ff).

In Deutschland gilt für die Leistungsflussdichte in den Frequenzbereichen von WLAN ein gesetzlicher Grenzwert von 10 W/m^2, der auf Empfehlungen der ICNIRP (International Committee on Non-Ionizing Radiation Protection) beruht. Es gibt jedoch Hinweise, dass elektromagnetische Strahlungen Schäden beim Menschen auch auf anderen Wegen hervorrufen können. Dies ist z. B. in einem Gutachten, das die Universität Bremen 2001 beim nova-Institut beauftragte, ausführlich dargestellt ([33]). In diesem Gutachten werden sogenannte Vorsorgegrenzwerte empfohlen, die bei 1/100 des gesetzlich vorgeschriebenen Grenzwerts liegen also bei 100 mW/m^2.

In dem Gutachten wurde nachgewiesen, dass WLAN Hotspots und Endgeräte bei regulärem Gebrauch selbst den Vorsorgegrenzwert in der Regel weit unterschreiten. So lag die Höchstbelastung durch Hotspots im untersuchten Bereich der Universität Bremen bei 0,025% des gesetzlichen und bei 2,5% des Vorsorgegrenzwerts. Belastungen, die durch Endgeräte (z. B. Laptops) verursacht sind, können dagegen wesentlich höher liegen. Bei 10 – 20 cm Abstand von der WLAN-Netzwerkkarte kann bei Volllastbetrieb der Vorsorgegrenzwert um bis zu 60% überschritten werden. Der eingehaltene Abstand ist jedoch im Allgemei-

nen größer und Volllast tritt nur selten auf. Der gesetzliche Grenzwert wird in jedem Fall weit unterschritten.

Im Vergleich mit WLAN sind Belastungen durch Mobilfunk und schnurlosen Telefonen (DECT-Geräte) i. d. R. größer. Das liegt zum einen an den höheren zugelassenen Sendeleistungen, zum anderen an einem geringeren Abstand der Anwender zu den Geräten. So beträgt die maximale Leistungsflussdichte von DECT-Geräten bei einem Abstand von 40 – 60 cm bereits ca. 170 mW/m^2 ([33]). Vor allem wegen des geringen Abstands sind Leistungsflussdichten von 500 – 1000 mW/m^2 bei Mobilfunkgeräten keine Ausnahme. Typische Werte von Strahlenimmissionen finden sich in [34], S. 41 und [35], S. 20.

Bei einer Nutzung von WLAN für die IP-Telefonie, die seit Kurzem technisch verfügbar ist, sind die Immissionswerte wegen des geringen Abstands allerdings ähnlich hoch wie beim Mobilfunk.

3.6 Existierende Konzepte für und Implementierungen von freier WLAN-Versorgung

Im Rahmen dieser Studie ist eine übergreifende Darstellung der existierenden freien WLAN-Versorgungen nicht möglich und wird auch nicht angestrebt. Anhand einiger ausgewählter Beispiele soll jedoch ein Überblick gegeben werden, der die Bandbreite der Realisierungsmöglichkeiten bezüglich unterschiedlicher Kategorien ersichtlich machen soll.

3.6.1 Anbieter, Motivationen und Zielsetzungen, Finanzierungsmodelle

Bei den Anbietern können folgende Kategorien unterschieden werden, die sich insbesondere auch durch die Motivation und die Zielsetzungen für den Betrieb von WLAN-Hotspots und -Netzen unterscheiden.

- Kommerzielle Anbieter: sie sind dadurch gekennzeichnet, dass sie einen kommerziellen Nutzen aus dem WLAN-Angebot ziehen wollen. Dabei kann zwischen einem direkten und einem indirekten Nutzen unterschieden werden:
  - Direkte Vermarktung: hierbei ist die Nutzung von WLAN-Hotspots nur oder überwiegend gegen Bezahlung möglich. Beispiele dafür sind die WLAN-Netze von Telekom Deutschland/FON, Kabel Deutschland etc.
  - Indirekte Vermarktung: der Nutzen besteht in Kundenbindung durch ein erhöhtes oder z. T. auch erwartetes Leistungsangebot und/oder dem damit verbundenen Imagegewinn. Beispiele dafür finden sich überwiegend in der Gastronomie (Cafés, Restaurants, Hotels) aber auch bei Verkehrsbetrieben (Busse, Bahn etc.).
- Freie Netze: es werden WLAN-Netze mit freiem Zugang angeboten. Die Motivation dafür ist, frei verfügbare Infrastruktur zu schaffen. Durch Kooperation, die auf private, freiwillige Beiträge setzt (Hotspots, gemeinsame Softwareentwicklung im Open-Source-Lizenzmodell), wird Infrastruktur für alle bereitgestellt. Ein Beispiel sind WLAN-Netze des Freifunks (freifunk.net) in Deutschland. Erklärtes Ziel ist u. a., eine Demokratisierung der Kommunikationsmedien zu bewirken ([36]).
- Kommunen, öffentliche Institutionen: hier sind im Wesentlichen drei Motive bzw. Zielsetzungen erkennbar:
  - Ausbau der Partizipationsmöglichkeiten durch öffentliche Infrastruktur
  - Steigerung der Attraktivität der Kommune für ihre Bürger und/oder für ihre Gäste
  - Förderung der lokalen Wirtschaft

  Öffentlich zugängliche Hotspots werden nicht nur auf öffentlichen Straßen und Plätzen angeboten, sondern auch in öffentlichen Einrichtungen wie Bürgerbüros, Bibliotheken u. ä.

Für die Finanzierung von freiem WLAN gibt es unterschiedliche Modelle:

- Von kommerziellen Anbietern wird freies WLAN als Lockangebot eingesetzt. Die Nutzung ist für eine begrenzte Zeit frei, danach werden Gebühren erhoben. Die Finanzierung erfolgt in diesem Fall als Werbekosten.
- Bei indirekter Vermarktung sind die Kosten als Infrarstruktur-Investitionen zu sehen.
- Das Teilnehmermodell, das die Telekom Deutschland zusammen mit der Firma FON anbietet, ist hier aufgeführt, obwohl es im eigentlichen Sinn nicht als kostenfreies WLAN betrachtet werden kann. Dabei stellen Kunden („Teilnehmer“), die einen Internetzugang des Anbieters nutzen, die freie Kapazität ihres WLAN-Routers öffentlich zur Verfügung. Die Nutzung dieses WLAN-Netzes ist für die Teilnehmer frei. Allen anderen wird eine kostenpflichtige Nutzung angeboten. Auch Kabel Deutschland bietet ein Teilnehmermodell an, das allerdings für alle 30 Minuten kostenfrei ist.
- In einigen Städten Deutschlands werden öffentliche, freie WLAN-Hotspots durch die Mitgliedsbeiträge von Vereinen finanziert, deren Mitglieder sich aus lokalen Wirtschaftsunternehmen, kommunalen Behörden und kommunalen Unternehmen zusammensetzen. Zusätzlich treten auch Sponsoren aus diesen Bereichen auf. Beispiel dafür ist die Stadt Pforzheim.
- Freifunknetze werden durch privates, nichtkommerzielles Engagement finanziert.
- Die Finanzierung öffentlichen, freien WLAN-Versorgung durch Kommunen erfolgt überwiegend auf folgenden Wegen:
  - durch direkte Finanzierung aus dem Haushalt. Beispiele sind die Städte Augsburg und Schweinfurt (s. Abschnitt 3.6.2).
  - durch kommunale Versorgungsunternehmen. Beispiele sind Unna (Investitionskosten 20.000 EUR) und Norderstedt.
  - durch Sponsoren, die teilweise kommunale Unternehmen sind. Beispiel ist München, wo das öffentliche WLAN-Netz durch das Portal muenchen.de und das kommunale Tochterunternehmen M-Net gesponsert wird.

Sowohl beim Angebot als auch bei der Finanzierung wird eine Vielzahl von Mischformen praktiziert.

3.6.2 Beispiele für öffentliche, kostenfreie WLAN-Versorgung in Deutschland

Kabel Deutschland bietet in Zusammenarbeit mit lokalen Betreibern deutschlandweit knapp 3000 Hotspots an. Der Zugang ist dort frei, das Login muss lediglich alle 30 Min. wiederholt werden. Darüber hinaus wird bei ca. 850 Hotspots auf öffentlichen Plätzen freier Zugang für 30 Min. am Tag angeboten ([37] und [38]).

Deutschlandweit bietet die Freifunk-Community über 10.000 Zugangspunkte an, die von privaten, nichtkommerziellen Anbietern auf freiwilliger Basis bereitgestellt werden ([39]).

In Berlin bietet Kabel Deutschland auf öffentlichen Plätzen 86 WLAN-Hotspots an ([38]), die 30 Min. pro Tag kostenfrei genutzt werden können. Das Projekt wurde von der Medienanstalt Berlin Brandenburg (MABB) mit 317.000 EUR unterstützt ([40]). Der Freifunk stellt ca. 400 Hotspots ([41]). Das Projekt wurde ebenfalls von der MABB mit 30.000 EUR gefördert ([42]).

Hamburg will die WLAN-Versorgung durch verschiedene kommerzielle Anbieter ausbauen. Neben Kabel Deutschland bietet auch die Telekom Deutschland seit Ende 2014 ca. 700 Hotspots für eine Stunde kostenfrei an ([43]). Die Installation von 7.000 Hotspots bis 2020 ist vom privaten Unternehmen willy.tel geplant ([44]). Das Projekt wird aus eigenen Mitteln finanziert. Es wird als Zukunftsinvestition bzw. Imagekampagne gesehen.

In Pforzheim wurde die Versorgung mit WLAN-Hotspots (52 Standorte) durch den Verein „Medien-/IT-Initiative Pforzheim“ initiiert ([45]), dem „führende Unternehmen aus der Medien-/IT-Branche in Pforzheim“ angehören. Der Ausbau bzw. der Betrieb des Netzes wurden/werden von der Stadt Pforzheim und dem Enzkreis mitfinanziert, Sponsor ist u. a. die Sparkasse Pforzheim Calw ([46]).

In Düsseldorf arbeitet die Stadt mit dem Unternehmen Wall AG zusammen, das WLAN in Zusammenhang mit der „Stadtmöblierung“ anbietet. Die Finanzierung erfolgt im Gesamtpaket und wird damit auch über Einnahmen der Werbeflächen der „Stadtmöblierung“ sichergestellt ([47]). Auch in Freiburg ist eine Zusammenarbeit mit der Wall AG geplant ([48]).

Die Stadt München bietet mit dem technischen Partner „Stadtwerke München“ ein WLAN-Netz mit derzeit 15 Hotspots an. Sponsoren sind die kommunalen Tochterunternehmen muenchen.de und M-Net ([49]).

Eine Versorgung durch kommunale Tochterunternehmen gibt es z. B. in Norderstedt und in Schweinfurt. In Norderstedt stellt das Kommunikationsunternehmen wilhelm.tel ein flächendeckendes WLAN-Netz mit derzeit knapp 500 Access-Points bereit ([50]), das von jedermann kostenfrei genutzt werden kann. Für Nutzer, die nicht Kunden von wilhelm.tel sind, gilt die Zugangsberechtigung nur jeweils 24 Std., kann aber ohne Einschränkungen jeweils für weitere 24 Std. erneuert werden ([51]). Die Stadt Schweinfurt finanziert ein Netz mit 10 Hotspots, das von dem kommunalen Tochterunternehmen RegioNet Schweinfurt GmbH aufgebaut und betrieben wird, mit 200 EUR pro Monat (Stand Ende 2014, [52] ab Min. 5:30).

In Augsburg wird ein kostenfreies öffentliches WLAN durch die Stadt finanziert. Augsburg hat mit dem Aufbau und dem Betrieb das private Unternehmen Stahl GmbH beauftragt ([53]).

In Unna wurde ein WLAN-Netz mit 24 Hotspots bereitgestellt, das im Auftrag der Stadtwerke vom privaten Unternehmen HeLi Net aufgebaut und betrieben wird ([54]). Es wird durch die Stadtwerke finanziert.

Um die Größenordnungen des bestehenden kommerziellen Angebots deutlich zu machen, seien hier die Teilnehmermodelle von Telekom Deutschland/FON und Kabel Deutschland genannt (s. Abschnitt 3.6.1), obwohl diese Netze nicht als kostenfrei gelten können. Das Netz von Kabel Deutschland hat deutschlandweit ca. 700.000 Hotspots ([37] und [38]), das von Telekom Deutschland/FON über 300.000 ([55]). Der Partner FON der Telekom Deutschland bietet nach eigenen Angaben weltweit über 14 Mio. Teilnehmer-Hotspots an ([56]).

3.6.3 Beispiele für öffentliche, kostenfreie WLAN-Versorgung im Ausland

Laut technikjournal.de ([57]) gilt: „Die in New York ansässige Firma für Marketing Forschung "ABI Research" zählte vergangenes Jahr 4,2 Millionen Hotspots weltweit. Davon befinden sich knapp 70 Prozent im asiatisch-pazifischen Raum und im Vergleich gerade mal neun Prozent in Europa. Im Westen sticht insbesondere das digitale Estland heraus. Hier gibt es kostenlos flächendeckendes WLAN, oft sogar mitten im Wald oder am Strand. Bis 2018 soll sich die Zahl auf 10,5 Millionen Hotspots weltweit erhöhen.“

Diese Zahlen umfassen eine sehr große Menge von privaten Hotspots, die unter Vertrag teilweise auch anderen Nutzern zur Verfügung stehen.

Einen groben Überblick über die Verbreitung von WLAN kann man beispielsweise durch Auswertung der Zahlen auf der Webpage von hotspot-locations.de erhalten:

Gebiet	Anzahl Hotspots in hotspot-locations.de
Weltweit	35299
Europa	18307
Nordamerika	12512
Asien	2860
Australien	472
Deutschland	6511

Tabelle 10 Anzahl Hotspots weltweit in verschiedenen Regionen (nach hotspot-locations.de)

Diese Zahlen sind zwar sicher nicht vollständig, können aber als Indikator für die relative geographische Verbreitung dienen.

Freifunknetze werden neben Deutschland auch in Österreich, der Schweiz und in Tschechien betrieben.

Eine ausführlichere Übersicht über kostenfreie WLAN-Versorgung im Ausland ist in der Tabelle im Abschnitt 8.2 enthalten.

3.6.4 WLAN im öffentlichen Verkehr

Flughäfen:

Folgende Tabelle 11 gibt eine Übersicht über das WLAN-Angebot auf den zehn größten deutschen Flughäfen gemäß Internetseiten der Flughäfen, Stand 10.06.2015:

Flughafen	Begrenzungen
Frankfurt (FRAU)	unbegrenzt
München (MUC)	unbegrenzt
Berlin Tegel / Schönefeld (TXL / SXF)	60 Min.
Düsseldorf (DUS)	30 Min.
Hamburg (HAM)	60 Min.
Stuttgart (STR)	60 Min.
Köln/Bonn (CGN)	unbegrenzt
Hannover (HAJ)	60 Min.
Nürnberg (NUE)	30 Min.
Bremen (BRE)	30 Min.

Tabelle 11 Kostenloses WLAN auf den 10 größten deutschen Flughäfen

Bahn:

Von der Deutschen Bahn werden WLAN-Hotspots – in Zusammenarbeit mit der Telekom Deutschland – auf dem größten Teil der ICE-Strecken angeboten. Kostenlos ist der Service derzeit nur in der 1. Klasse, in der 2. Klasse gelten die Hotspot-Tarife der Telekom Deutschland ([58]).

Laut einem Bericht der Welt ([59]) ist seitens der Deutschen Bahn (DB) geplant, kostenloses WLAN ab Mitte 2016 auch in der 2. Klasse bereit zu stellen. In dem Bericht heißt es weiter, dass für die Einführung von WLAN in allen anderen Zügen der DB keine konkreten Pläne bestehen. WLAN in Regionalzügen und S-Bahnen wird es in nennenswertem Umfang in frühestens fünf Jahren geben. Auch die neuen ICs, die ab 2017 schrittweise in Dienst gestellt werden, werden für WLAN lediglich vorgerüstet. Vereinzelt soll WLAN auch davor in einigen Regionalzügen angeboten werden, z. B. ab Ende 2015 im Elektronetz-Niedersachsen-Ost (ENNO) und ab 2018 in Zügen des Rhein-Ruhr-Express (RRX).

U-Bahn, Nahverkehrsbusse:

Ein existierendes Angebot und konkrete Planungen für WLAN gibt es im Hamburger Verkehrsverbund ([60]). Seit Ende 2012 wird dort auf zwei Buslinien WLAN angeboten, die Einführung in weiteren Linien ist geplant. Die 2013 angekündigte Einführung von WLAN in den U-Bahnen wurde jedoch zwischenzeitlich wieder aufgegeben ([44]). WLAN in Stadtbussen gibt es auch in Lippe ([61]).

In München hat die Stadt Mitte 2014 entschieden, keine WLAN-Versorgung im öffentlichen Nahverkehr aufzubauen ([62]).

Bahnhöfe und Haltestellen:

Die Deutsche Bahn bietet an 127 ihrer ca. 5400 Bahnhöfe und Haltestellen kostenloses WLAN an. Die Nutzungsdauer ist auf 30 Min. beschränkt ([63]). Ein Beispiel für kostenfreie öffentliche Hotspots an Haltestellen ist das Angebot der AKN Eisenbahn AG (Altona-Kaltenkirchen-Neumünster, [64]).

Fernbusse:

Laut Focus online ([65]) haben fast alle großen Fernbuslinien in Deutschland bereits WLAN in den Bussen installiert. Die Anbindung an das Internet erfolgt über Mobilfunk, überwiegend über UMTS in wachsendem Maße auch über LTE. Bei UMTS-Anbindung ist Zahl der Nutzer beschränkt (8 oder 16). Wegen Lücken in der Mobilfunkversorgung, insbesondere bei LTE ist die Zuverlässigkeit der Verbindungen derzeit begrenzt ([66]).

Schiffe:

Auf Initiative der bayerischen Staatsregierung wurde der Aufbau einer WLAN-Versorgung auf Schiffen der Bayerischen Seenschifffahrt auf dem Starnberger See gestartet ([67]). Die Anbindung erfolgt über Standard-Mobilfunkverbindungen.

3.6.5 Freifunk

Freifunk bietet für die öffentliche Hand einen alternativen Weg, WLAN-Versorgung im großen Stil zu fördern und die Verbreitung von freiem WLAN erheblich zu beschleunigen. Freifunk-Netze, die kostenlose WLAN-Versorgung anbieten, gibt es auch im Ausland, z. B. in Österreich, in der Schweiz und in Tschechien ([68]).

Im Gegensatz zur herkömmlichen Nutzung von WLAN-Routern, die über DSL ans Internet angebunden werden, erfolgt bei Freifunk die Anbindung einer großen Zahl von Nutzern über private, kostenlose Richtfunkstrecken. Das heißt, dass mit Hilfe von Freifunk das WLAN-Versorgungsgebiet erheblich vergrößert werden kann. Voraussetzung dafür ist allerdings, dass weitere Mitglieder für Freifunk gewonnen werden.

In Deutschland ist die Versorgung mit kostenlosem WLAN durch Freifunknetze (Stand Anfang 2015) wie folgt ([69]):

- 10.145 Freifunk Knoten (Access Points)
- 145 Initiativen (Vereine, Meshed-Netze)
- Verkehr am Berliner Freifunk-Uplink: 190 MBit/s
- Datenvolumen im Januar 2015 am Berliner Freifunk-Uplink: 67 TeraByte.

Wenn man diese Zahlen betrachtet, dann ist es verwunderlich, dass Freifunk in der Öffentlichkeit kaum bekannt ist. In der vorgenannten Quelle wird auch das erhebliche Wachstum der Freifunkbewegung über die Zeit dargestellt.

Um ein besseres Verständnis der Freifunk-Thematik zu vermitteln fassen wir hier die Charakteristik der Freifunk-Netze und der Freifunk-Bewegung kurz zusammen:

- Die Hotspots der Freifunknetze werden fast immer per Richtfunkstrecken miteinander verbunden zu sogenannten Meshed-Netzen. Die Richtfunkstrecken sind im WLAN-Frequenzbereich, limitiert auf Distanzen bis zu 10 km, meist jedoch nur wenige hundert Meter lang.
- Die Einspeisung ins Internet, bzw. der Zugang zum Internet erfolgt teilweise über Peering-Points im Ausland (Schweden), teils über vereinseigene DSL-Anschlüsse.
- Freifunk-Netze basieren meistens auf Low-Cost Hardware, die sehr kostengünstig von Herstellen verfügbar ist, die zumeist in Asien produzieren.
- Die Software auf diesen Geräten wird soweit als irgend möglich komplett ersetzt durch Open Source Software, die zum Teil auch in den jeweiligen Vereinen selbst programmiert oder angepasst wurde (Änderungen werden wieder als Open Source veröffentlicht).
- die Ethik der beteiligten Personen ist beeinflusst von der „Hacker-Ethik“ des Chaos Comupter Club (CCC, [70]) und von den Ideen der Amateurfunk-Bewegung.
- der harte Kern der Freifunk-Bewegung sind Open-Source- und Funk-Experten, die sehr detaillierte technische Kenntnisse über IT- und HF-Technik haben.
- Sämtliche Firmware wird nur in Form von Open Source verwendet. Closed Source Firmware wird strikt abgelehnt, weil man Backdoors befürchtet.
- In manchen Ländern liefert die Freifunkbewegung einen Zugang zum Internet, der von den Behörden nicht oder nur sehr schwer kontrolliert werden kann.
- Freifunker sehen ihre Netze auch als eine Infrastruktur die unabhängig von anderen Netzen im Katastrophenfall genutzt werden kann.
- Durch Verhandlungen mit dem WLAN-Geräte-Herstellern hat man sehr niedrige Preise bei hohen Stückzahlen erzielt.
- Teilweise kommen sogar selbst gebaute Router bzw. Outdoor-WLAN-Geräte für Richtfunkstrecken zum Einsatz.

Die Richtfunkstrecken nutzen vielfach öffentliche Gebäude und hohe Dachstandorte der Mitglieder der Freifunk-Organisationen.

Vielerorts wurden und werden die Freifunknetze von Gemeinden und in Berlin auch durch die Medienanstalt Berlin-Brandenburg mit öffentlichen Geldern gefördert.

Nach uns vorliegenden Informationen sind die Freifunk-Netze technisch meist auf einem sehr guten Stand, allerdings bei Verwendung sehr kostengünstiger Geräte. Durch zusätzliche öffentliche Förderung könnten Freifunknetze erheblich höhere Bandbreiten unterstützen. Die eingesetzten Methoden und ein Großteil der Software sind sowohl bei Low-Cost, als auch bei höherwertigen Geräten einsetzbar.

Allerdings ist für die Unterstützung leistungsfähigerer Hardware in gewissem Umfang die Anpassung zusätzlicher Treiber oder zusätzlicher Funktionen notwendig. Diesbezügliche Details zu klären führt über den Rahmen dieser Studie hinaus.

4 Zielsetzungen

4.1 Aspekte mobiler Internetnutzung

4.1.1 Mobile Internetanwendungen und deren Nutzung

Laut der Online-Studie 2014 von ARD und ZDF ([71], Mobile Nutzung/Mobile Onlineanwendungen) sind die Anwendungen der mobilen Internetnutzung, geordnet nach dem Prozentsatz der sie nutzenden Anwender, folgende:

Anwendung	Prozentsatz der Anwender
Kommunikation	77
E-Mail	40
Facebook	38
Allgemeine Infos/Recherchen/Suchmaschinen	38
WhatsApp	35
Navigation/Ortungsdienste/Routenplaner/Kartenfunktionen	27
aktuelle Serviceinfos (Wetter/Verkehr)	26
aktuelle Nachrichten/News/Onlinezeitungen	21
Videos/Videodownloads	10
Sportseiten	8
Radio bzw. Musik hören	8
Onlinespiele	8
sonstige Onlinecommunitys	7
sonstige Messenger	7
Reise- bzw. Fahrplanauskünfte	6
Shoppen	5
Wissensportale/Übersetzer	4
Berufliches/Geschäftliches/Universität etc.	3
Touristische Infos	3
Geschäfts-/Restaurantsuche	3
Onlinebanking	3
Fernsehprogramme	3
Kommunikation/Infoaustausch (allg.)	2
Produktsuche/Preisvergleiche	2
Fotos/Bilderdownloads	2
Unterhaltung/Zeitvertreib	2
Kulturelles/Veranstaltungstipps etc.	1
Adresssuche	1
App-Suche	1
Telefonbuch/Rufnummernsuche	0

Tabelle 12 Anwendungen der mobilen Internetnutzung

Eine herausragende Stellung nimmt die direkte Kommunikation mit anderen Internetteilnehmern ein (Kommunikation, E-Mail, Facebook, WhatsApp), gefolgt von Informationsdiensten, die teilweise einen direkten Bezug zum Bedarf des Anwenders vermuten lassen (allgemeine Infos/Recherchen/Suchmaschinen, Navigation/Ortungsdienste/Routenplaner/Kartenfunktionen, aktuelle Serviceinfos (Wetter/Verkehr), aktuelle Nachrichten/News/Onlinezeitungen). Unterhaltung, touristische und kommerzielle Anwendungen nehmen eine untergeordnete Stellung ein.

In dieser Statistik ist keine Standortabhängigkeit berücksichtigt. Es ist anzunehmen, dass z. B. touristische Informationen an touristischen Brennpunkten einen wesentlich höheren Anteil an der Nutzung haben oder Reise- und Fahrplanauskünfte an Bahnhöfen, Flughäfen etc.

4.1.2 Nutzergruppen und -orte

Allgemein verfügbar sind Statistiken zu mobiler Internetnutzung bezüglich Altersgruppen. In nachfolgender Tabelle 13 ist der Anteil der jeweiligen Altersgruppe nach Erhebungen der ard-zdf-onlinestudie.de aufgeführt ([71]).

	Gesamt	14 – 19 J	20 – 29 J	30 – 39 J	40 – 49 J	50 – 59 J	Ab 60 J
Gelegentlich	50	77	74	66	42	32	21
Täglich	22	46	48	31	12	8	2

Tabelle 13 Mobile Internetnutzung 2014 nach Altersgruppen (ard-zdf-onlinestudie.de)

Im Rahmen dieser Studie wurden keine Statistiken zur Internetnutzung durch andere gesellschaftliche Gruppierungen (z. B. Studenten, Rentner etc.) ausgewertet. Dies gilt ebenso für statistische Daten zur örtlichen Verteilung der Anwendungen und Nutzergruppen.

Örtlichkeiten, die für eine kostenfreie öffentliche WLAN-Versorgung in Frage kommen, sind in folgender Liste aufgeführt:

- Stark frequentierte öffentliche Plätze und Straßen
- Bahnhöfe, Haltestellen des öffentlichen (Nah-)Verkehrs
- Ämter, Behörden
- Krankenhäuser
- Alten- und Pflegeheime
- Bildungseinrichtungen und Kulturstätten: Bibliotheken, Museen, Denkmäler
- Schulen: Gymnasien, Hochschulen
- Einkaufscenter
- Freizeiteinrichtungen: Schwimmbäder, Sportstätten, Veranstaltungsorte

4.2 Versorgungsziele kommunaler und staatlicher Stellen

4.2.1 Kostenfreies WLAN im Kontext der Grundversorgung

In Deutschland besteht gemäß Telekommunikationsgesetz ein Grundversorgungsanspruch „auf Anschluss an ein öffentliches Telekommunikationsnetz und auf einen Zugang zu öffentlich zugänglichen Telefondiensten“, der derzeit durch die Telekom Deutschland GmbH sichergestellt wird. Ein Grundversorgungsanspruch für einen breitbandigen Internetanschluss besteht hingegen nicht ([72]).

Innerhalb der EU wird diskutiert, ob der Breitband-Internetzugang in den Grundversorgungskatalog aufgenommen werden muss. In Deutschland wird mit der Breitbandstrategie der Bundesregierung eine gegenüber dem jetzigen Stand stark verbesserte Versorgung angestrebt. Sie ist aber nicht gesetzlich verankert ([73]). In der Schweiz wurde der breitbandige Internetzugang als öffentlicher Dienst bereits 2008 in den gesetzlich geregelten Leistungskatalog der Grundversorgung aufgenommen ([73],[74], [75]).

Leistungen der Grundversorgung, wie z. B. die medizinische Grundversorgung, das Verkehrs- und Beförderungswesen, Gas/Wasser/Elektrizität, Bildung, Postzustellung, Rundfunk etc. stehen den Bürgern nur teilweise kostenlos zur Verfügung. Im Wesentlichen kostenfrei sind z. B. Verkehrswege und Bildungseinrichtungen. Wasser-, und Energieversorgung, öffentliche Verkehrsmittel, Telekommunikation und Post, Müllabfuhr, kulturelle Einrichtungen etc. müssen in Abhängigkeit von den bezogenen Leistungen bezahlt werden. Um die Grundversorgung in diesen Fällen auch für Bedürftige sicherzustellen, werden die Aufwendungen dafür grundsätzlich in den Sozialhilfesätzen berücksichtigt. Zudem gibt es für viele Leistungen Ermäßigungen oder eine Kostenbefreiung für bestimmte Gruppen, wie z. B. für Behinderte im öffentlichen Personennahverkehr.

Im Zusammenhang mit der Diskussion über einen Grundversorgungsanspruch auf Breitbandzugang in Europa steht die Kostenpflichtigkeit nicht zur Debatte. Vor diesem Hintergrund ist ein Grundversorgungsanspruch auf kostenfreies WLAN nur schwer begründbar. Ein

solches Angebot wird aus Sicht der Autoren eine freiwillige Leistung der jeweiligen kommunalen oder staatlichen Institutionen bleiben.

4.2.2 Mögliche Versorgungsziele

Wie bereits in Abschnitt 3.6.1 festgestellt wurde, können für kommunale und staatliche Stellen im Wesentlichen drei Versorgungsziele identifiziert werden. Diese Ziele überschneiden sich teilweise, spielen aber auch zusammen:

1. Bereitstellung allgemein zugänglicher Infrastruktur, um möglichst breiten Bevölkerungskreisen Teilhabe zu ermöglichen
2. Erhöhung der Attraktivität der Kommune bzw. der Region
3. Förderung der Wirtschaft

Wie in Abschnitt 3.6.2 dargestellt wurde, arbeiten Kommunen bei der Bereitstellung einer freien WLAN-Versorgung oft mit kommerziellen Anbietern zusammen mit dem Ziel, eigene Ausgaben zu minimieren. Der Beitrag der Kommunen besteht dann im Wesentlichen darin, WLAN-Netze politisch zu unterstützen, teilweise werden kommerziellen Anbietern auch Anreize wie z. B. kostenfreie oder günstige Standorte, befristete freie Stromversorgung o. ä. angeboten.

Mit einem solchen Ansatz werden evtl. die Zielsetzungen 2 und 3 erreicht. Bezüglich der Bereitstellung einer allgemein zugänglichen Infrastruktur besteht jedoch i. d. R. ein Zielkonflikt mit dem Kooperationspartner, der durch die in Abschnitt 3.6.1 beschriebenen unterschiedlichen Zielsetzungen bedingt ist. Beispielhaft dafür ist Berlin, wo mehrfach Versuche solcher Kooperationen unternommen wurden, die jedoch bisher scheiterten ([40], [76]). Ende 2014 wurde ein neuer Anlauf gestartet, in dem Berlin erstmalig einen finanziellen Beitrag leisten will – in Höhe von 170.000 EUR ([76]). Von einer flächendeckenden Versorgung ist man abgerückt ([77]).

Will die Politik die Zielsetzung 1 erreichen, ist eine Einflussnahme auf die Standortauswahl, verfügbare Kapazitäten und Zugangsbedingungen erforderlich. Gestaltungsspielraum in dieser Hinsicht kann i. d. R. nur durch ein finanzielles Engagement geschaffen werden. Wie die in Abschnitt 3.6.2 beschriebenen Beispiele zeigen, hängt die Höhe der erforderlichen Mittel sehr stark von den gegebenen Rahmenbedingungen ab. Z. B. hat eine Kommune mit einem kommunalen Tochterunternehmen, das über ein eigenes Breitbandkabelnetz verfügt, i. A. einen erheblichen Kostenvorteil. Wie das Beispiel Norderstedt zeigt, kann eine flächendeckende und mit hohen Datenraten ausgestattete WLAN-Versorgung dann sogar ohne finanziellen Beitrag der Kommune erreicht werden.

5 Umsetzungskonzepte für kostenfreies WLAN in Bayern

Im Folgenden werden Konzepte zur Förderung bzw. Einführung von kostenfreiem öffentlichen WLAN im Freistaat Bayern vorgeschlagen. Für einige der Konzepte wäre ein abgestimmtes Vorgehen mehrerer oder aller Bundesländer auch mit Beteiligung des Bundes ableitbar.

Die Konzepte betreffen die Versorgung

- im öffentlichen Raum
- in Bildungseinrichtungen und Kulturstätten
- in öffentlichen Verkehrsmitteln
- durch nichtkommerzielle, private Initiativen (Freifunk)

Die Konzepte beinhalten größtenteils jeweils Schemata zur Kostenkalkulation und beispielhafte Kostenberechnungen. Weil die Rahmenbedingungen noch offen sind und Einzelkosten

nicht zuverlässig geschätzt werden können, sind die Beispielrechnungen nicht belastbar und können lediglich Größenordnungen der zu erwartenden Kosten wiedergeben.

5.1 Konzept 1: Freie WLAN-Versorgung im öffentlichen Raum

5.1.1 Umsetzungsstrategien

Zur Förderung kommunaler WLAN-Versorgung können folgende Maßnahmen ergriffen werden:

- Finanzielle Förderung der Gemeinden bei der Einrichtung einer WLAN-Versorgung
  - Einmaliger Zuschuss bei der Einrichtung von WLAN-Hotspots
  - Zuschuss zu den laufenden Kosten

  Zuschüsse können als fixer Betrag oder als prozentualer Anteil der jeweiligen Kosten gegeben werden.
- Kommerzielle Unterstützung durch Rahmenverträge mit
  - Anbietern von Festnetzanschlüssen (DSL, VDSL)
  - Anbietern von Mobilfunkanschlüssen (GSM, UMTS, LTE)
  - Hard- und Softwareanbietern
  - Installationsfirmen

  Rahmenverträge können regional aber auch landesweit abgeschlossen werden. Möglich sind Ausschreibungen, die jeweils zeitlich begrenzt einen Rahmenvertrag mit nur jeweils einem Anbieter beinhalten. Durch Rahmenverträge begünstigt sind der Freistaat Bayern, die bayerischen Kommunen und ggf. weitere staatliche Stellen, die WLAN-Versorgung bereitstellen.
- Logistische Unterstützung durch ein Zentrum des Landes (z. B. IT-Dienstleistungszentrum des Freistaats Bayern) bezüglich:
  - Installationsberatung
  - Bereitstellung von Hardware und Firmware
  - Sicherheits-Infrastruktur: Authentifizierungsserver, VPN-Server etc.

  Die Installationsberatung beinhaltet Lösungsvorschläge (best practices) für unterschiedliche Versorgungszwecke. Ähnlich der Freifunk-Community kann die Behörde Hardware, Software und Firmware bereitstellen. Die Bereitstellung von Sicherheitsinfrastruktur würde es den Kommunen ermöglichen, sichere WLAN-Hotspots einzurichten.

  Denkbar ist auch eine Zusammenarbeit mit der Freifunk-Community insbesondere bezüglich der Nutzung von Software/Firmware, die dort unter Open Source Lizenz verfügbar ist, wie dies z. B. in Meerbusch geplant wurde ([78]). Dabei verwendet die Kommune die Infrastruktur, die von der Freifunk-Community bereitgestellt wird (kostengünstige Router, Zugangs- und Vernetzungssoftware (s. auch Abschnitt 5.4).

Förderung der Wirtschaft:

- Bereitstellung einer Infrastruktur für geschäftsmäßige WLAN-Betreiber, die kostenfreies öffentliches WLAN bereitstellen, z. B.:
  - Bereitstellung von Hardware und Firmware
  - Authentifizierungs-Server
  - VPN-Server

5.1.2 Kostenschätzungen

Wie in Abschnitt 4.1.1 beschrieben, werden Internetanwendung in der mobilen Nutzung überwiegend für Kommunikation und Auskunftsdienste (allgemeine Suchanfragen, Navigation/Ortung, Wetter/Verkehr, Nachrichten) verwendet. Auch wenn für einzelne dieser Anwendungen örtliche Schwerpunkte vermutet werden können (z. B. aktuelle Fahrpläne/Verspätungen an Bahnhöfen und Flughäfen), ist es im Rahmen dieser Studie wegen der erforderlichen Datenerhebungen zu aufwändig, Kriterien für die Versorgung an diesen Nutzungen auszurichten. Als Kriterium wird daher die Nutzerreichweite herangezogen, die auf Grundlage von Gemeindestatistiken abgeschätzt wird.

Zur Abschätzung der Kosten wird ein Kalkulationsschema in MS Excel bereitgestellt. Zur Verbesserung der Übersicht werden Einmalkosten in monatliche Amortisationsbeiträge umgerechnet (bei festzulegenden Amortisationszeiten und –zinsen). Das Schema beinhaltet:

- die Berechnung der durchschnittlichen monatlichen Kosten pro WLAN-Hotspot aus
  - einmaligen Einrichtungskosten und deren Umrechnung in monatliche Raten über festzulegende Amortisationszeiträume und –zinsen. Eingabegrößen sind:
    - Hardwarekosten
    - Installationskosten
    - Anschlussgebühren
    - Amortisationszeitraum
    - Amortisationszinsen
  - monatlichen Unterhaltskosten. Eingabegrößen sind:
    - Wartungskosten
    - Anschlussgebühren
- die Berechnung der Anzahl der Hotspots für eine bayernweite Versorgung auf Basis von Gemeindestatistiken. Eingabegrößen sind:
  - die Größe der Gemeinde, ab der eine WLAN-Versorgung bereitgestellt wird
  - die durchschnittliche Zahl der Hotspots pro 1.000.000 Einwohner

Die Kalkulation kann für die Versorgungskategorien „In Gebäuden“ und „Im Freien“ mit jeweils unterschiedlichen Eingabegrößen durchgeführt werden, deren Resultate zu einem Gesamtergebnis zusammengeführt werden. Die Kosten für den Freistaat Bayern werden aus den Gesamtkosten durch Anwendung eines Fördersatzes bestimmt.

Tabelle 14 und Tabelle 15 enthalten die Kalkulation für unterschiedliche Versorgungsdichten pro 1 Mio. Einwohner, nämlich für 200/500 und 300/800 (in Gebäuden/im Freien) bei gleichen Kosten pro Hotspot.

Die Kosten pro Hotspot sind grob geschätzt und können zuverlässig erst nach Einholung von Angeboten bzw. nach Abschluss von Rahmenverträgen bestimmt werden.

Die Anzahl der erforderlichen Hotspots wird als Summe der erforderlichen Hotspots der Kommunen berechnet, deren Einwohnerzahl größer gleich dem Parameter „ab EW“ ist. Pro Kommune wird die Anzahl aus der Einwohnerzahl und dem Parameter „HS/1Mio.EW“ (Hotspots pro 1 Mio. Einwohner) berechnet (nach oben gerundet).

Kategorie	Leistung	In Gebäuden	Im Freien	Gesamt
Anzahl	HS /1Mio.EW	200	500	
	ab EW	2.000	20.000	
Anzahl ges.		2.926	2.442	
Fixkosten	Hardware	150,00 €	800,00 €	
	Installation	120,00 €	2.500,00 €	
	Anschluss	50,00 €	120,00 €	
Amortisation	Laufzeit [Mon.]	24	24	
	Zins [%]	5	5	
	mntl. Kosten	14,04 €	150,04 €	
Mntl. Kosten	Wartung	10,00 €	20,00 €	
	Anschluss	30,00 €	30,00 €	
Kosten pro HS	Mntl. Kosten	54,04 €	200,04 €	
Kosten gesamt	Mntl.	158.117,66 €	488.498,05 €	646.615,71 €
	Jährl.	1.897.411,92 €	5.861.976,64 €	7.759.388,55 €
Kosten Freistaat	Fördersatz	60 %		4.655.633,13 €

Tabelle 14 Kalkulation Beispiel 1

Kategorie	Parameter	In Gebäuden	Im Freien	Gesamt
Anzahl	HS /1Mio.EW	300	800	
	ab EW	1.000	10.000	
Anzahl ges.		4.672	5.662	
Fixkosten	Hardware	150,00 €	800,00 €	
	Installation	120,00 €	2.500,00 €	
	Anschluss	50,00 €	120,00 €	
Amortisation	Laufzeit [Mon.]	24	24	
	Zins [%]	5	5	
	mntl. Kosten	14,04 €	150,04 €	
Mntl. Kosten	Wartung	10,00 €	20,00 €	
	Anschluss	30,00 €	30,00 €	
Kosten pro HS	Mntl. Kosten	54,04 €	200,04 €	
Kosten gesamt	Mntl.	252.469,48 €	1.132.627,35 €	1.385.096,83 €
	Jährl.	3.029.633,79 €	13.591.528,15 €	16.621.161,94 €
Kosten Freistaat	Fördersatz	60 %		9.972.697,16 €

Tabelle 15 Kalkulation Beispiel 2

5.1.3 Synergien

Eine mehrfach genutzte Möglichkeit, öffentliches kostenfreies WLAN kostengünstig bereitzustellen, ist der Weg über kommunale Versorgungsunternehmen. Insbesondere wenn diese auf dem Gebiet der Kommunikation tätig sind und in diesem Zusammenhang bereits über Breitband-Kabelnetze verfügen, können Synergieeffekte genutzt werden:

- Die Anbindung der Hotspots an das Breitbandkabelnetz kann sehr günstig bereitgestellt werden, eine flächendeckende Versorgung ist grundsätzlich möglich.
- Ein Ausgleich zwischen Gemeinwohl und Gewinnerzielungsinteressen ist bei kommunalen Unternehmen leichter zu erreichen, da der Eigentümer überwiegend Gemeinwohlinteressen vertritt.

Beispiele für die Bereitstellung von öffentlichen, kostenfreien WLAN-Netzen in Zusammenarbeit mit kommunalen Kommunikationsunternehmen sind die Städte Norderstedt, München und Schweinfurt. Diese Möglichkeit steht jedoch nur wenigen Kommunen zur Verfügung.

5.2 Konzept 2: Förderung von freiem WLAN in Bildungseinrichtungen und Kulturstätten

5.2.1 Hintergründe

In Zusammenhang mit Schulen und Hochschulen ist unter dem Begriff „öffentliches WLAN" der Zugang aller Angehörigen (Schüler, Studenten, Lehrkräfte und sonstige Angestellte) dieser Institute zu verstehen.

An den bayerischen Hochschulen ist kostenfreies, öffentliches WLAN omnipräsent. Allein im Münchner Wissenschaftsnetz des Leibniz Rechenzentrums gibt es 2758 WLAN-Accesspoints ([79]). Auch die Universität mit der kleinsten Anzahl Studierender in Bayern, die Katholische Universität Eichstätt/Ingolstadt, bietet ihren Studenten über 50 Accesspoints in Eichstätt und weitere 25 in Ingolstadt an ([80], [81]).

Während öffentliches WLAN an Hochschulen weitgehend unumstritten ist, gibt es bezüglich der Einführung an Schulen Diskussionen. Diese beziehen sich zum einen auf mögliche Gesundheitsschäden durch Strahlenbelastung (s. z. B. [82]). Generell werden aber auch die Vor- und Nachteile digitaler Medien im Unterricht diskutiert. Laut einer forsa-Umfrage überwiegen nach Ansicht bayerischer Lehrer deren Vorteile im Unterricht die Nachteile leicht. Eine Mehrheit der Lehrer hält jedoch den Einsatz mobiler Endgeräte für jeden Schüler für eher überflüssig (51%), während nur 41% ihn für sinnvoll halten ([83], S. 12ff). Die Themen „Strahlenbelastung" und „Einsatz digitaler Medien im Unterricht" werden im Rahmen dieser Studie nicht behandelt.

5.2.2 Umsetzungskonzepte

Angesichts der oben dargestellten Situation der WLAN-Versorgung im Bereich der Hochschulen wird davon ausgegangen, dass hier keine über die bestehenden hinausgehenden Fördermaßnahmen erforderlich sind.

Zur Förderung der WLAN-Versorgung in Schulen, Museen und Denkmälern werden dieselben Konzepte vorgeschlagen wie die in Abschnitt 5.1.1 genannten Konzepte zur Förderung kommunaler WLAN-Versorgung, wobei der Begriff „Kommunen" durch „Schulträger" zu ersetzten ist. Soweit der Freistaat für die Finanzierung selbst zuständig ist, ist der Begriff „Zuschuss" jeweils durch „Finanzierung" zu ersetzen.

5.2.3 Kostenschätzungen

Kostenschätzungen können nach dem gleichen Kalkulationsschema wie in Abschnitt 5.1.2 durchgeführt werden. Lediglich die Anzahl der erforderlichen Hotspots ist anders zu bestimmen.

Die Anzahl der erforderlichen WLAN-Router an Schulen hängt wesentlich davon ab, welcher Versorgungsgrad erreicht werden soll. Hierfür kommen folgende Ansätze in Frage:

1. Versorgung beschränkt auf die Lehrkräfte
2. Versorgung in eigenen Computer-Lehrräumen
3. Versorgung in allen Klassenzimmern

Im Fall 2 gibt es Empfehlungen, Netzanschlüsse nicht über Funk sondern über Kabel herzustellen, um die Strahlenbelastung zu reduzieren (s. Abschnitt 5.2.1).

Folgende Tabelle 16 enthält die Anzahl der Schulen in Bayern im Herbst 2013 ([84]):

Schulart	Schulen	Klassen
Grund- sowie Mittel-/Hauptschulen.	3 337	30 161
davon Grundschulen	2 406	19 781
Mittel-/Hauptschulen	1 023	10 380
Förderzentren	351	5 005
Realschulen	374	9 060
Realschulen zur sonderpäd. Förderung	4	71
Abendrealschulen	4	20
Gymnasien	422	10 231
Abendgymnasien	5	28
Kollegs	6	42
Schulen besonderer Art	3	104
Freie Waldorfschulen	21	333
Sonstige allgemeinbildenden Schulen	8	186
Zusammen	**4 535**	**55 241**

Tabelle 16 Anzahl der Schulen in Bayern im Herbst 2013

Für die Schulen in Bayern kann eine Kostenkalkulation gemäß den drei genannten Versorgungsansätzen durchgeführt werden. Es wird eine Amortisationszeit von 5 Jahren (60 Monate) unterstellt.

Kategorie	Leistung	Nur Lehrkräfte	Computer-räume	Alle Klassen-zimmer
Anzahl ges.		4500	10000	55000
Fixkosten	Hardware	150,00 €	150,00 €	150,00 €
	Installation	120,00 €	120,00 €	120,00 €
	Anschluss	50,00 €	50,00 €	50,00 €
Amortisation	Laufzeit [Mon.]	60	60	60
	Zins [%]	5	5	5
	mntl. Kosten	6,04 €	6,04 €	6,04 €
Mntl. Kosten	Wartung	10,00 €	10,00 €	10,00 €
	Anschluss	30,00 €	30,00 €	30,00 €
Kosten / HS	Mntl. Kosten	46,04 €	46,04 €	46,04 €
Kosten gesamt	Mntl.	207.174,58 €	460.387,95 €	2.739.308,29 €
	Jährl.	2.486.094,92 €	5.524.655,37 €	32.871.699,46 €

Tabelle 17 Kosten der WLAN-Versorgung in bayerischen Schulen

Bei der Berechnung der Anzahl der WLAN-Router im Fall spezieller Computerräume wurde ein Computerraum pro 10 Klassen unterstellt. Es sind also 5.500 Computerräume und 4.500 Lehrerzimmer auszurüsten.

Im Fall einer Versorgung pro Klasse kommen zu den ca. 55.000 Klassenzimmern 4.500 Lehrerzimmer.

Laut Wikipedia gibt es in Bayern 1.153 Museen ([85]). Die Anzahl der Router, die pro Museum erforderlich wäre, wurde im Rahmen dieser Studie nicht ermittelt. Unterstellt man einen Durchschnitt von 3 WLAN-Routern pro Museum, ergibt sich folgende Kalkulation:

Kategorie	Leistung	Museen
Anzahl ges.		3450
Fixkosten	Hardware	150,00 €
	Installation	120,00 €
	Anschluss	50,00 €
Amortisation	Laufzeit [Mon.]	60
	Zins [%]	5
	mntl. Kosten	6,04 €
Mntl. Kosten	Wartung	10,00 €
	Anschluss	30,00 €
Kosten / HS	Mntl. Kosten	46,04 €
Kosten gesamt	Mntl.	158.833,84 €
	Jährl.	1.906.006,10 €

Tabelle 18 Kosten der WLAN-Versorgung in bayerischen Museen

5.3 Konzept 3: Förderung von freiem WLAN im öffentlichen Nahverkehr

5.3.1 Hintergründe

Ein WLAN-Hotspot in einem Fahrzeug des öffentlichen Verkehrs muss über Mobilfunk an das Internet angeschlossen werden. Das bedeutet, dass die erzielbaren Datenraten im Wesentlichen von der Qualität der Mobilfunkversorgung in den Regionen abhängen, in denen das jeweilige Fahrzeug eingesetzt ist.

Aus Sicht der Mobilfunkbetreiber lohnt sich ein Ausbau der Versorgung der Schienennetze i. d. R. nicht. Eine Funkzelle deckt einen Gleisabschnitt von nur wenigen Kilometern ab. Ein Zug durchfährt diesen in wenigen Minuten. Abhängig von der Frequenz der Züge ist die Zelle den größten Teil der Zeit nicht genutzt. Nach Aussage von Mobilfunkbetreibern „spiele [das] kaum die Stromkosten ein." ([86]).

Eine vollständige Versorgung von Bahnstrecken müsste daher bei Mobilfunkbetreibern bezuschusst oder bestellt werden. Bezüglich der ICE-Strecken in Deutschland gibt es Bestrebungen in diese Richtung ([87]).

Ein wesentlicher Parameter für die Qualität der Internetverbindung ist die Anzahl der Nutzer im jeweiligen Verkehrsmittel. Z. B. können in Fernbussen bei einer LTE-Mobilfunkverbindung alle Fahrgäste ausreichend mit WLAN versorgt werden. Besteht nur eine 3G-Verbindung (UMTS, HSPA), ist die Anzahl der Nutzer auf 8 - 16 beschränkt (s. Abschnitt 3.6.4). Den ca. 50 – 80 Sitzplätzen im Bus stehen jedoch bis zu 1200 Sitzplätze in einem ICE und mehrere hundert in einem Nahverkehrszug gegenüber, von denen selbst bei einer guten LTE-Verbindung nur ca. 100 – 200 gleichzeitig mit WLAN versorgt werden können. Werden Anwendungen mit höheren Datenraten (z. B. Video) verwendet, so sinkt die Anzahl der Nutzer auf ca. 20 – 30 (s. Tabelle 7) pro Zug.

Die Schweizer Bundesbahn (SBB) hat sich aus grundsätzlichen Gründen gegen die Einführung von WLAN in ihren Zügen entschieden. Sie fördert mobile Internetverbindungen in Ihren Zügen durch den Einbau von Signalverstärkern für alle Mobilfunksysteme (2G, 3G, 4G). Durch Zusammenarbeit mit den Mobilfunkbetreibern ist in der Schweiz die Abdeckung des Schienennetzes wesentlich besser als in Deutschland ([88]). Mit diesen beiden Maßnahmen weist die mobile Internetnutzung in Schweizer Bahnen in einen vergleichsweise hohen Standard aus.

Die Entscheidung gegen die Einführung von WLAN wird damit begründet, dass damit die Übertragungskapazitäten nicht erhöht würden, jedoch nach Fahrgastbefragungen die Daten-

volumina bei kostenfreiem WLAN erheblich steigen würden. Die Kosten für diese Verbindungen hätten dann nicht die Nutzer sondern die SBB und damit die Allgemeinheit zu tragen. Das würde eine Subventionierung von Mobilfunkdiensten bedeuten, die die SBB ablehne ([89]).

5.3.2 Umsetzungskonzepte

Die Einführung von WLAN in Fernverkehrszügen liegt nicht im Einflussbereich der Bundesländer. Auf Ebene der Länder – und darunter – betreffen Fördermaßnahmen in erster Linie den öffentlichen Personennahverkehr (ÖPNV). Für die Organisation des ÖPNV in Bayern ist zum einen der Freistaat als Aufgabenträger des Schienenpersonennahverkehrs (SPNV) zuständig. Er hat damit die Bayerische Eisenbahngesellschaft mbH (BEG) beauftragt, die die Leistungen plant, Verkehrsunternehmen damit beauftragt und deren Leistungserbringung überwacht ([90]).

Zum anderen organisieren Kommunen darüber hinaus kommunalen und auch kommunenübergreifenden ÖPNV, der i. d. R. aus Busverkehr besteht. Sie werden bei dieser Aufgabe vom Land bezuschusst.

Die im Folgenden aufgeführten Fördermaßnahmen sind nach den unterschiedlichen Zuständigkeiten aufgegliedert:

SPNV:

Die Einführung von WLAN kann mit zwei Maßnahmen gefördert werden:

- Die Planung und Finanzierung der WLAN-Versorgung durch die BEG nach Vorgaben des Landtags bzw. der Staatsregierung
- Eine Kooperation mit den Mobilfunkbetreibern, um die Versorgung der Bahnlinien in ausreichender Qualität sicherzustellen.

Zum Punkt 2 gibt es derzeit einen runden Tisch, an dem die Mobilfunkanbieter, die Besteller und Nahverkehrsunternehmen gemeinsam erarbeiten, wo und wie der WLAN-Empfang verbessert werden muss ([91]).

Die Höhe der Finanzierung des SPNV wird auf Bundesebene entschieden. Seitens der Aufgabenträger wird beklagt, dass die bereitgestellten Mittel nicht ausreichten, den Nahverkehr in seinem derzeitigen Umfang beizubehalten ([92]). Sollte der Bund keine wesentliche Erhöhung der Mittel für den SPNV beschließen, ist die Finanzierung von kostenfreiem WLAN in Nahverkehrszügen aus diesen Mitteln schwer begründbar. Allerdings könnte Freistaat Mittel aus dem eigenen Etat bereitstellen. Angesichts des Investitionsbedarfs an anderer Stelle bestünde aber auch hier Begründungsbedarf.

Kommunal organisierter ÖPNV:

- Die Bezuschussung von WLAN-Projekten durch den Freistaat

5.3.3 Kostenschätzungen

Zu den Kosten einer WLAN-Versorgung in Zügen gibt es widersprüchliche Daten. Während im Verkehrsministerium von Sachsen-Anhalt die Ausrüstung eines Elektrotriebwagens mit WLAN auf 75.000 EUR geschätzt wird ([93]), meint ein Sprecher des Rhein-Main-Verkehrsverbunds, dass die Frage nach den Kosten einer Ausrüstung der Nahverkehrszüge „derzeit nicht seriös beantwortet werden [könne]“ ([94]). Allgemein ist die Ausrüstung neuer Fahrzeuge erheblich kostengünstiger als die Nachrüstung in alten Fahrzeugen ([94], [59]).

Bezüglich der Anzahl der auszurüstenden Verkehrsmittel sind in nachfolgender Tabelle 19 beispielhaft die Daten des Münchner MVVs angeführt ([95]).

Verkehrsmittel	Anzahl
S-Bahn	244
U-Bahn	508
Tram	91
Innerstädtische Busse	422
Regionale Busse	468

Tabelle 19 Anzahl der Fahrzeuge je Verkehrsmittel im Münchner Verkehrsverbund (MVV)

Ein Beispiel für eine Kalkulation der Kosten für die Ausrüstung aller Fahrzeuge im MVV mit WLAN ist in folgender Tabelle 20 gegeben. Sie weist jährliche Kosten in Höhe von ca. 5,6 Mio. EUR aus. In der Kalkulation stellen die Installationskosten den wesentlichen Anteil. Da sie derzeit nicht seriös ermittelt werden können, ist die Kalkulation fiktiv.

Kategorie	Leistung	S-Bahn	U-Bahn	Tram	Bus	Gesamt
Anzahl ges.		244	508	91	890	
Fixkosten	Hardware	500,00 €	500,00 €	500,00 €	500,00 €	
	Installation	25.000,00 €	25.000,00 €	25.000,00 €	25.000,00 €	
	Anschluss	50,00 €	50,00 €	50,00 €	50,00 €	
Amortisation	Laufzeit [Mon.]	120	120	120	96	
	Zins [%]	5	5	5	5	
	mntl. Kosten	271,00 €	271,00 €	196,75 €	158,88 €	
Mntl. Kosten	Wartung	30,00 €	30,00 €	30,00 €	30,00 €	
	Anschluss	30,00 €	30,00 €	30,00 €	30,00 €	
Kosten / HS	Mntl. Kosten	331,00 €	331,00 €	256,75 €	218,88 €	
Kosten gesamt	Mntl.	80.763,36 €	168.146,67 €	23.364,39 €	194.804,98 €	467.079,40 €
	Jährl.	969.160,36 €	2.017.760,10 €	280.372,67 €	2.337.659,72 €	5.604.952,85 €

Tabelle 20 Fiktive Kalkulation der monatlichen und jährlichen Kosten für WLAN im MVV

5.4 Konzept 4: Förderung einer privaten, nichtkommerziellen freien WLAN-Versorgung bzw. Vernetzung

Unter der Prämisse, dass die Störerhaftung entfällt, ist für die weitere Förderung einer privaten, nichtkommerziellen freien WLAN-Versorgung folgende Vorgehensweise am geeignetsten:

1. Bekanntmachung der Möglichkeiten von WLAN und des Freifunk-Konzeptes durch
   - gezielte, professionelle Videos, die das Prinzip Freifunk und die Möglichkeiten die dadurch entstehen, erläutern und einer großen Personengruppe bekannt machen.
   - Veranstaltungen mit dem gleichen Ziel, zum Beispiel in
     - IHKs
     - Volkshochschulen
     - Universitäten
     - Fachhochschulen
     - Landratsämtern
     - Stadtverwaltungen
     - Gemeinden
     - Gymnasien
     - etc.
2. Parallel:
   - Bereitstellung von gut dokumentierten best practice Beispielen in Zusammenarbeit mit ausgewählten Freifunk-Gruppen und Open Source Vereinen, z.B.
     - Open Source Business Alliance (OSBA)
     - Free Software Foundation (FSF)

6 Literaturverzeichnis

[1] TÜV Rheinland - BMVI, „Bericht zum Breitbandatlas Ende 2014," 2014. [Online]. Available: http://www.zukunft-breitband.de/SharedDocs/DE/Anlage/Digitales/bericht-zum-breitbandatlas-ende-2014-ergebnisse.pdf?__blob=publicationFile.

[2] Wikipedia, „Störerhaftung - Internetrecht," 2015. [Online]. Available: http://de.wikipedia.org/wiki/St%C3%B6rerhaftung#Internetrecht.

[3] Video Stream Hosting, „Einstellungen und Hinweise für Videostreaming," [Online]. Available: http://www.video-stream-hosting.com/beratung-support/technische-tipps/.

[4] Wikipedia, „Datenübertragungsrate - Video- und Audiosignale," [Online]. Available: http://de.wikipedia.org/wiki/Daten%C3%BCbertragungsrate#Video-_und_Audiosignale.

[5] skype, „Wie viel Bandbreite braucht Skype?," 2015. [Online]. Available: https://support.skype.com/de/faq/FA1417/wie-viel-bandbreite-braucht-skype.

[6] connect, „Wieviel Datenvolumen verbrauchen Facebook, Youtube & E-Mail?," 2015. [Online]. Available: http://www.connect.de/ratgeber/datenvolumen-facebook-youtube-whatsapp-ausland-roaming-surfen-2469005.html.

[7] Verivox, „Wie viel Datenvolumen brauche ich wofür?," 2015. [Online]. Available: http://www.verivox.de/ratgeber/wie-viel-datenvolumen-brauche-ich-wofuer-85845.aspx.

[8] Datentarife.net, „Datenvolumen," [Online]. Available: http://www.datentarife.net/ratgeber/datenvolumen/#.VW6wmVLkp44.

[9] Wikipedia, „Digital Subscriber Line," 2015. [Online]. Available: http://de.wikipedia.org/wiki/Digital_Subscriber_Line#Bandbreite.2C_Daten.C3.BCbertragungsrate_und_D.C3.A4mpfung.

[10] glasfaser-internet.info, „Glasfaser Anbieter im Überblick," 2015. [Online]. Available: http://www.glasfaser-internet.info/anbieter/glasfaser-anbieter-uebersicht.html.

[11] GLASFASER-Internet, „Glasfaser Anbieter im Überblick," 2015. [Online]. Available: http://www.glasfaser-internet.info/anbieter/glasfaser-anbieter-uebersicht.html.

[12] Elektronik Kompendium, „Datenübertragung im Mobilfunk," [Online]. Available: http://www.elektronik-kompendium.de/sites/kom/0910141.htm.

[13] Wikipedia, „Wireless Local Area Network, Datenübertragungsraten," 2015. [Online]. Available: http://de.wikipedia.org/wiki/Wireless_Local_Area_Network#Daten.C3.BCbertragungsraten.

[14] Elektronik Kompendium, „IEEE 802.16 / WiMAX," [Online]. Available: http://www.elektronik-kompendium.de/sites/net/0904211.htm.

[15] ITM Informationstransport und -management GmbH, „Richtfunk-Übersicht," [Online]. Available: http://www.itm-group.com/web/richtfunk.html.

[16] J. Hansryd und J. Edstam, „Microwave capacity evolution," Ericson Review 1 2011, 2011.

[17] H. Karcher, „LTE-Bandbreite: Warum kommen keine 100 Megabit/s?," ZDNet, 20. November 2012. [Online]. Available: http://www.zdnet.de/88132147/lte-bandbreite-warum-kommen-keine-100-mbits-einflussfaktoren-der-4g-surfgeschwindigkeit/.

[18] A. Spier, „Darf's ein bisschen schneller sein? Wie sich LTE im mobilen Alltag schlägt," c't, 2012. [Online]. Available: http://www.heise.de/ct/artikel/Darf-s-ein-bisschen-schneller-sein-1722006.html.

[19] Elektronik Kompendium, „Glasfaser-Netzarchitektur," [Online]. Available: http://www.elektronik-kompendium.de/sites/kom/1403191.htm.

[20] freifunk.net, „WLAN-Antennen," 2013. [Online]. Available: https://wiki.freifunk.net/WLAN-Antennen.

[21] Wiki LEIPZIG.FREIFUNK.NET, „Antennenreichweite," 2012. [Online]. Available: http://wiki.leipzig.freifunk.net/Antennenreichweite.

[22] Bundesnetzagentur, *Allgemeinzuteilung von Frequenzen für die Nutzung in lokalen Netzwerken; Wireless Local Area Networks (WLAN- Funkanwendungen),* Bundesnetzagentur, 2013.

[23] Bundesnetzagentur, *Allgemeinzuteilung von Frequenzen in den Bereichen 5150 MHz - 5350 MHz und 5470 MHz - 5725 MHz für Funkanwendungen zur breitbandigen Datenübertragung, WAS/WLAN („Wireless Access Systems including Wireless Local Area Networks"),* Bundesnetzagentur, 2010.

[24] J. M. Scott und J. Burns, „Study on Impact of traffic off-loading and related technological trends on the demand for wireless broadband spectrum," 2013.

[25] BMJV, „Telemediengesetz (TMG), § 8," 26. 02. 2007. [Online]. Available: http://www.gesetze-im-internet.de/tmg/__8.html.

[26] R. Mantz, Rechtsfragen offener Netze, Karlsruhe: Universitätsverlag Karlsruhe, 2008.

[27] M. Behling, „Freifunk-Freedom-Fighter-Box gegen Störerhaftung und Abmahnwahn," Freifunkblog, 15. 06. 2012. [Online]. Available: http://blog.freifunk.net/2012/freifunkfreedomfighterbox-gegen-st%C3%B6rerhaftung-und-abmahnwahn.

[28] Freifunk Franken - Wiki, „Freifunk-Gateway aufsetzen," 2015. [Online]. Available: https://wiki.freifunk-franken.de/w/Freifunk-Gateway_aufsetzen.

[29] Deutschlandfunk, „Angst vor Public WLAN," 06. 07. 2013. [Online]. Available: http://www.deutschlandfunk.de/angst-vor-public-wlan.684.de.html?dram:article_id=252130.

[30] Wikipedia, „FON, Rechtliche Lage," 2014. [Online]. Available: http://de.wikipedia.org/wiki/FON#Rechtliche_Lage.

[31] heise online, „fon und 1&1 legen Rechtstreit um WLAN-Sharing bei," 21. 06. 2011. [Online]. Available: http://www.heise.de/newsticker/meldung/fon-und-1-1-legen-Rechtstreit-um-WLAN-Sharing-bei-1264681.html.

[32] J. Rech, Wireless LANs, Hannover: Heise Zeitschriften Verlag GmbH & Co. KG, 2012.

[33] nova-Institut für Ökologie und Innovation - EMF-Abteilung, „Gutachten zur Feststellung der Belastung durch hochfrequente elektromagnetische Strahlung durch Funk-Netzwerke an der Universität Bremen," Bremen, 2001.

[34] M. Wuschek und C. Bornkessel, „Hochfrequenz-Immissionen durch funkbasierte Breitbanddienste," Industrie und Handelskammer für München und Oberbayern, 2007.

[35] C. Mehnert, „Elektromagnetische Felder durch Mobilfunk," Bayerisches Landesamt für Umwelt (LfU), 2012.

[36] freifunk.net, „Worum geht's," [Online]. Available: http://freifunk.net/worum-geht-es/.

[37] Kabel Deutschland, „So einfach gehts:," 2015. [Online]. Available: http://www.kabeldeutschland.de/wlan-hotspots/so-einfach-gehts.html.

[38] Kabel Deutschland, „Mit dem Hotspotfinder von Kabel Deutschland finden Sie den nächsten Hotspot in Ihrer Nähe," 2015. [Online]. Available: http://www.kabeldeutschland.de/wlan-hotspots/hotspots-finden.html.

[39] Freifunk.net, „Community finden," 2015. [Online]. Available: http://freifunk.net/wie-mache-ich-mit/community-finden/.

[40] Berliner Zeitung, „Senat plant kostenloses WLAN in Berlin," 16. 10. 2014. [Online]. Available: http://www.berliner-zeitung.de/berlin/einfuehrung-anfang-2015-geplant-senat-plant-kostenloses-wlan-in-berlin,10809148,28750564.html.

[41] Freifunk Berlin, „OpenWiFiMap," 2015. [Online]. Available: http://berlin.freifunk.net/network/map/.

[42] freifunk.net, „Neues Setup verstärkt Berliner Freifunk-Netz," [Online]. Available: http://freifunk.net/blog/2013/11/berlin-backbone-erweiterung-neues-setup-auf-dem-bezirksamt-kreuzberg-verstaerkt-berliner-freifunk-netz/.

[43] Telekom Deutschland, „Telekom macht Hamburg zum Surferparadies," [Online]. Available: http://www.hotspot.de/content/news_tcity2.html.

[44] Die Welt, „Hamburg wird zur WLAN-Hauptstadt," 16. 11. 2014. [Online]. Available: http://www.welt.de/regionales/hamburg/article134356792/Hamburg-wird-zur-WLAN-Hauptstadt.html.

[45] Medien-/IT-Initiative Pforzheim e. V., „Medien-/IT-Initiative Pforzheim e.V.," [Online]. Available: http://www.mit-pf.de/.

[46] Stadt Pforzheim, „Pforzheim erste deutsche Großstadt mit freiem WLAN," September 2013. [Online]. Available: http://www.pforzheim.de/buerger/aktuelles-presse/pressemeldungen/s1/article/3822.html.

[47] www.tarif4you.de, „Düsseldorf: Kostenlose WLAN-Hotspots in der Innenstadt," 2013. [Online]. Available: http://www.tarif4you.de/news/n17809.html.

[48] invidis consulting GmbH, „Freies WLAN für Freiburg – Wall AG stattet aus," Januar 2015. [Online]. Available: http://invidis.de/2015/01/aussenwerberechte-freies-wlan-fuer-freiburg-wall-ag-stattet-aus/.

[49] muenchen.de, „WLAN Hotspots in München," 2015. [Online]. Available: http://www.muenchen.de/leben/wlan-hotspot.html.

[50] willy.tel, „MobyKlick Karte," 2015. [Online]. Available: http://www.mobyklick.de/index.php?id=availability.

[51] willy.tel, „MobyKlick Hilfe," 2015. [Online]. Available: http://www.mobyklick.de/index.php?id=help.

[52] SW-N.TV, „Kostenloses W-LAN in der Innenstadt von Schweinfurt - SW-N.TV (YouTube)," 22. 12. 2014. [Online]. Available: https://www.youtube.com/watch?v=OeQkH8oz2ts.

[53] Stadt Augsburg, „WLAN – Surfen im Stadtgebiet," 2015. [Online]. Available: http://www.augsburg.de/buergerservice-rathaus/buergerservice/wlan/.

[54] Stadtwerke Unna, „UNglaublich: Der größte Hotspot im Ruhrgebiet funkt in Unna," 2014. [Online]. Available: http://www.sw-unna.de/service/aktuelles/news/article/unglaublich-der-groesste-hotspot-im-ruhrgebiet-funkt-in-unna/.

[55] Telekom Deutschland, „HotSpot – so funktioniert's," 2015. [Online]. Available: http://www.hotspot.de/.

[56] FON, „Your Global WiFi Network," 2015. [Online]. Available: https://corp.fon.com/en#what_is_fon.

[57] technikjournal.de, „Öffentliche Hotspots versorgen Bonn mit Internet," 19. 01. 2015. [Online]. Available: http://www.technikjournal.de/cms/front_content.php?idcatart=1755idcat=59.

[58] DB Bahn, „HotSpot im ICE – die beste Verbindung von Mobilität und Internet," [Online]. Available: http://www.bahn.de/p/view/service/zug/railnet_ice_bahnhof.shtml.

[59] Die Welt, „WLAN im Zug bleibt ein Luxus für wenige Bahnfahrer," 15. 03. 2015. [Online]. Available: http://www.welt.de/wirtschaft/article138899388/WLAN-im-Zug-bleibt-ein-Luxus-fuer-wenige-Bahnfahrer.html.

[60] Nahverkehr Hamburg, „Internet in Bus und Bahn," [Online]. Available: http://www.nahverkehrhamburg.de/hvv/internet-in-bus-und-bahn-themenseite.

[61] Lippe mobil, „Kostenfreies WLAN im Bus," Mai 2014. [Online]. Available: http://www.kvg-lippe.de/de/aktuelles.

[62] Bayerischer Rundfunk, „Stadt sagt Nein zu WLAN in Bus und Bahn," 20. 06. 2014. [Online]. Available: http://www.br.de/nachrichten/oberbayern/wlan-muenchen-bus-u-bahn-tram-100.html.

[63] DB Bahn, „30 Minuten gratis WLAN an über 120 Bahnhöfen," [Online]. Available: http://www.bahn.de/p/view/service/bahnhof/railnet_bahnhof.shtml.

[64] wilhelm.tel, „WLAN-Netz MobyKlick jetzt an allen AKN-Haltestellen verfügbar," [Online]. Available: http://www.wilhelm-tel.de/privatkunden/service/aktuelles/wlan-netz-mobyklick-jetzt-an-allen-akn-haltestellen-verfuegbar/.

[65] Focus, „Fernbus: Gratis-WLAN für Fahrgäste," 2014. [Online]. Available: http://www.focus.de/digital/handy/so-schnell-surfen-sie-auf-reisen-fernbus-gratis-wlan-fuer-fahrgaeste_id_3861107.html.

[66] fernbusse.de, „Pluspunkt Internet: Kostenloses WLAN im Fernbus," 28. 05. 2014. [Online]. Available: http://www.fernbusse.de/aktuelles/kostenloses-wlan-im-fernbus-1400/.

[67] Bayerisches Staatsministerium der Finanzen für Landesentwicklung und Heimat, *SÖDER: KOSTENFREIES SURFEN AUF DEM STARNBERGER SEE,* 2015.

[68] Wikipedia, „Freifunk," 2015. [Online]. Available: https://de.wikipedia.org/wiki/Freifunk.

[69] C. E. Achele, H. Dr. Hege, T. Kleinz, H. Lahmann und D. Pachall, „WLAN FÜR ALLE, Freie Funknetze in der Praxis," Februar 2015. [Online]. Available: http://mabb.de/files/content/document/Publikationen/Freifunk-Broschuere/freifunk_publikation_webversion_2.Auflage.pdf.pdf.

[70] CCC Chaos Computer Club, „Hackerethik," [Online]. Available: http://www.ccc.de/de/hackerethik.

[71] ard-zdf-onlinestudie.de, „ard-zdf-onlinestudie.de," 05. 09. 2014. [Online]. Available: http://www.ard-zdf-onlinestudie.de.

[72] Bundesnetzagentur, „Grundversorgung mit Teilnehmeranschlüssen," 06. 06. 2014. [Online]. Available: http://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Verbraucher/WeitereThemen/GrundversorgungmitTeilnehmeranschluessen/GrundversorgungMitTeilnehmeranschluessen-node.html.

[73] Wikipedia, „Grundversorgung, Breitbandzugang," 2015. [Online]. Available: http://de.wikipedia.org/wiki/Grundversorgung#Breitbandzugang.

[74] Schweizer Bundesamt für Kommunikation, „Grundversorgung im Fernmeldebereich," 02. 02. 2015. [Online]. Available: http://www.bakom.admin.ch/themen/telekom/00457/index.html?lang=de.

[75] heise online, „Schweizer Regierung erhöht Vorgaben für Internet-Grundversorgung," [Online]. Available: http://www.heise.de/newsticker/meldung/Schweizer-Regierung-erhoeht-Vorgaben-fuer-Internet-Grundversorgung-2443416.html.

[76] heise online, „Öffentliches WLAN: Berlin schreibt Gebäude als Hotspot-Standort aus," 01. 12. 2014. [Online]. Available: http://www.heise.de/newsticker/meldung/Oeffentliches-WLAN-Berlin-schreibt-Gebaeude-als-Hotspot-Standort-aus-2469874.html.

[77] RBB - Radio Berlin Brandenburg, „Freies WLAN für alle – aber erst ab Herbst 2016," 06. 05. 2015. [Online]. Available: http://www.rbb-online.de/politik/thema/2015/republica2015/beitraege/freies-wlan-fuer-alle.html.

[78] RP online, „Politiker entscheiden über Gratis-WLAN," 22. 04. 2015. [Online]. Available: http://www.rp-online.de/nrw/staedte/meerbusch/politiker-entscheiden-ueber-gratis-wlan-aid-1.5033785.

[79] Leibniz Rechenzentrum, „Überblick über das Münchner Wissenschaftsnetz (MWN), WLAN," 2015. [Online]. Available: https://www.lrz.de/services/netz/mwn-ueberblick/#top7.

[80] Katholische Universität Eichstätt-Ingolstadt, „Zugang zum Hochschulnetz - WLAN, VPN, Intranet," [Online]. Available: http://www.ku.de/rechenzentrum/it-services/netz/.

[81] Katholische Universität Eichstätt-Ingolstadt, „Funknetz [WLAN],“ [Online]. Available: http://www.ku.de/rechenzentrum/it-services/netz/wlan/.

[82] Die Welt, „Bundesamt warnt Schulen vor WLAN-Netzen,“ 19. 02. 2015. [Online]. Available: http://www.welt.de/gesundheit/article137612666/Bundesamt-warnt-Schulen-vor-WLAN-Netzen.html.

[83] forsa Institut, „IT an Schulen - Ergebnisse einer Repräsentativbefragung von Lehrern in Deutschland,“ 06. 11. 2014. [Online]. Available: http://www.bllv.de/fileadmin/Dateien/Land-PDF/Wissenschaft/Forsa_ITanSchulen14__Bayern.pdf.

[84] Bayerisches Landesamt für Statistik, „Eckdaten der amtlichen Schulstatistik in Bayern im Herbst 2013 nach kreisfreien Städten und Landkreisen,“ 2013. [Online]. Available: https://www.statistik.bayern.de/medien/statistik/bildungsoziales/schu_eckdaten-bayern_2013.pdf.

[85] Wikipedia, „Museen in Deutschland - Museen nach Land,“ [Online]. Available: http://de.wikipedia.org/wiki/Museen_in_Deutschland#Museen_nach_Land.

[86] W. Kempkens, „Das Handy bleibt in Regionalzügen zu oft stumm,“ ingenieur.de, 12. 11. 2013. [Online]. Available: http://www.ingenieur.de/Themen/Bus-Bahn/Das-Handy-bleibt-in-Regionalzuegen-zu-oft-stumm.

[87] C. Schlesiger, „Bald LTE in jedem ICE,“ Wirtschaftswoche, 29. 12. 2014. [Online]. Available: http://www.wiwo.de/unternehmen/dienstleister/mobilfunk-offensive-der-bahn-bald-lte-in-jedem-ice/11166990.html.

[88] P. Beuth, „Nur ein Provider bietet "sehr gute" Netzabdeckung,“ Zeit Online, 03. 12. 2014. [Online]. Available: http://www.zeit.de/digital/mobil/2014-12/netzabdeckung-deutschland-mobilfunk-vergleich-connect-2014.

[89] SBB, „Unterwegs verbunden – Hintergrundinfos zu den Mobilfunkservices.,“ [Online]. Available: http://www.sbb.ch/sbb-konzern/medien/dossier-medienschaffende/unterwegs-verbunden.html#5.

[90] BEG (Bayerische Eisenbahngesellschaft mbH), „Aufgaben,“ 2015. [Online]. Available: http://beg.bahnland-bayern.de/die-beg/aufgaben.

[91] Deutsche Bahn, „Pressekonferenz zur Digitalisierung bei der Deutschen Bahn,“ 05. 06. 2015. [Online]. Available: http://www.deutschebahn.com/file/de/3223632/4z8IFbrEJ3CqQaGlSlA4nR635Xs/9367336/data/rede_grube_pk_digitalisierung.pdf.

[92] BAG-SPNV, „Schriftliche Stellungnahme der BAG: Entwurf eines Dritten Gesetzes zur Änderung des Regionalisierungsgesetzes,“ 23. 02. 2015. [Online]. Available: http://www.bundestag.de/blob/361182/4470491ed28717718b967fd9003b335b/031_stellungnahme_bag-spnv-data.pdf.

[93] R. Jensen, „WLAN im Nahverkehr lässt auf sich warten,“ Kieler Nachrichten, 30. 03. 2015. [Online]. Available: http://www.kn-online.de/News/Aktuelle-Nachrichten-Wirtschaft/News-Aktuelle-Nachrichten-Wirtschaft/WLAN-im-Nahverkehr-laesst-auf-sich-warten.

[94] web.de, „WLAN im Nahverkehr lässt auf sich warten,“ 30. 03. 2015. [Online]. Available: http://web.de/magazine/digital/wlan-nahverkehr-laesst-warten-30545726.

[95] MVV - Münchner Verkehrs- und Tarifverbund, „Daten, Zahlen, Fakten,“ 2015. [Online]. Available: http://www.mvv-muenchen.de/de/der-mvv/mvv-in-zahlen/.

[96] K. Landefeld, „Verbreitung und Nutzbarkeit von WLAN, WLAN-Zugangspunkten sowie öffentlicher Hotspots in Deutschland,“ Verband der deutschen Internetwirtschaft e. V., Berlin, 2014.

[97] Surf-Stick.net, „Datenvolumen,“ [Online]. Available: http://www.surf-stick.net/datenvolumen.html.

[98] CHIP Digital GmbH, „WLAN-Router im Test - Bestenliste,“ 2015. [Online]. Available: http://www.chip.de/bestenlisten/Bestenliste-WLAN-Router--index/extended/id/1138/.

[99] P. Stamm und F. Büllingen, „Stellenwert und Marktperspektiven öffentlicher sowie privater Funknetze im Kontext steigender Nachfrage nach nomadischer und mobiler hochbitratiger Datenübertragung," WIK, Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste, Bad Honef, 2014.

[100] Cisco, „Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2014–2019," 2015.

[101] Bundesnetzagentur, „Jahresbericht 2014," 2015.

[102] B. Theiss, „Mobilfunk im Zug," *connect Spezial,* 2014.

[103] Premail Services, „wireless hotspots," [Online]. Available: http://hotspots.primail.ch/.

7 Anhang

7.1 Telemediengesetz

7.1.1 § 7 Allgemeine Grundsätze

(1) Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

(2) Diensteanbieter im Sinne der §§ 8 bis 10 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt. Das Fernmeldegeheimnis nach § 88 des Telekommunikationsgesetzes ist zu wahren.

7.1.2 § 8 Durchleitung von Informationen

(1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie

- die Übermittlung nicht veranlasst,
- den Adressaten der übermittelten Informationen nicht ausgewählt und
- die übermittelten Informationen nicht ausgewählt oder verändert haben.

Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

(2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.

7.2 Kostenfreies öffentliches WLAN in Deutschland

Folgende gibt eine beispielhafte Übersicht über kostenfreies öffentliches WLAN in deutschen Kommunen

Ort	Betreiber	Anzahl HS	Nutzergruppen	Finanzierung	Registrierung	Beschränkungen
Augsburg	Stahl GmbH	9 Standorte	Jeder	??	Akz. Nutzer-Bed.	500 MB/Tag
Berlin	Kabel D, Medienanstalt Berlin-Brandenburg Hotsplots, QSC AG, Freifunk	162	Jeder	Kabel D, MABB (317.000) Zuschuss Miet- u. Stromkosten (170.000)	Akz. Nutzer-Bed.	30 Min.
Berlin	Freifunk	385	Jeder	Private Teilnehmer	Akz. Nutzer-Bed.	30 Min.
Düsseldorf	Wall AG	52	Jeder	Werbung, Querfinanzierung Stadtmöblierung	Vorname, Name, E-Mail	Keine
Freiburg	Wall AG	Geplant	Jeder	Werbung, Querfinanzierung Stadtmöblierung	Vorname, Name, E-Mail	Keine
Hamburg	Initiative privater Anbieter	700 Telekom 62 Kabel D 7000 willy.tel (gepl.)	Jeder	Verschiedene Anbieter (Stadt will möglichst wenig finanzieren)	Unterschiedlich	Unterschiedlich
München	M-Net	14	Jeder	muenchen.de, M-Net	Akz. Nutzer-Bed.	Neuanmeldung jeweils nach 1 Std.
Norderstedt	willhelm.tell	621	Einwohner, Gäste	Willhelm.tel (Tochter der Stadtwerke)	E-Mail, Passwort	Keine
Pforzheim	Verein	52	Jeder	Sparkasse, Stadt, Wirtschaftsunternehmen, Enzkreis, IHK	Vorname, Name, E-Mail, Mob.Nr./ Paypal, Passwort	500 MB/Monat
Schweinfurt	RegioNet Schweinfurt GmbH	10	Jeder	Stadt (200 EUR/Mon.)	Akz. Nutzer-Bed.	2 Std.
Unna	SW Unna, HeliNet	24	Kunden von SW/HeliNet, Gastzugang	SW Unna, HeliNet	Login, Passwort, Akz. Nutzer-Bed.	30 Min. für Gäste

Tabelle 21 Kostenfreies öffentliches WLAN in deutschen Kommunen

7.3 Kostenfreies öffentliches WLAN im Ausland

Einen guten Überblick über die verfügbaren Hotspots gibt folgende Webpage (*): http://www.hotspot-locations.com/

Überblick USA auch: http://www.wififreespot.com/

Überblick des internationalen WLAN-Anbieters Fon: https://corp.fon.com/de

Angeblich werden von fon weltweit 14,7 Millionen WLAN-Router zur Verfügung gestellt.

Es gibt auch Apps, die das Auffinden von kostenlosen Apps vereinfachen, z.B.:
https://itunes.apple.com/de/app/free-wi-fi-finder/id307217005?mt=8

Folgende Tabelle 22 gibt einen beispielhaften Überblick über kostenfreies öffentliches WLAN im Ausland

Kontinent	Land	Beschreibung	Besonderheiten
Europa	England	WLAN hat eine große Verbreitung. London spannte für die Olympischen Sommerspiele 2012 über die Stadtteile Kensington, Chelsea und Westminster das größte freie WLAN-Netz Europas und bot auch darüber hinaus in allen Londoner U-Bahn-Stationen freien Zugang an.	Offene, kostenfreie Hotspots sind die Regel, wobei aber abweichend davon in Hotels oft nur kostenpflichtige Hotspots verfügbar sind.
Europa	Russland	In Moskau gibt es einige öffentliche Hotspots. Nach Angaben des Tourismusportals sind in der Stadt Moskau nun alle zwölf Linien der Metro mit kostenlosem WLAN ausgestattet werden.	Die Situation in Moskau kann nicht auf ganz Russland übertragen werden.
Europa	Österreich	WLAN wird hier häufig durch Stadtverwaltungen installiert und betreiben (Beispiel Linz). Auch regionale Netzbetreiber haben WLAN Hotspots eingerichtet. Mittlerweile ist Linz mit 120 Hotspots im Verhältnis zu der Einwohnerzahl Spitzenreiter in Europa.	
Europa	Estland	Estland gilt als Vorreiter in Sachen WLAN. In fast jeder estnischen Stadt gibt es mindestens einen Hotspot, der die Bewohner mit WLAN versorgt. Das Hotspot-Netzwerk Wifi.ee, über das Privatpersonen nicht genutztes Datenvolumen weitergeben können, deckt eine Fläche ab, die fast so groß wie das Land selbst ist.	

Kontinent	Land	Beschreibung	Besonderheiten
Europa	Schweiz	Die Schweizer Bundesbahnen haben Hotspots in fast allen Bahnhöfen installiert. Es besteht ein geregelter Zugang wobei die Freischaltung der Nutzer über SMS erfolgt. Es gibt eine Vielzahl regionaler Anbieter von WLAN-Hotspots.	Die Erfassung der Zugangsdaten ist gesetzlich vorgeschrieben.
Europa	Italien	Im WLAN-Verzeichnis sind derzeit etwa 360 Hotspots in ganz Italien registriert, davon ca. 16% kostenlos. In Rom sind angeblich 500 Hotspots an öffentlichen Orten verfügbar (Stand 2011)	Laut Veröffentlichung von 2011 sollen 4200 Handwerksbetriebe einen WLAN Hotspot öffentlich zur Verfügung stellen. Auch alle großen Campingplatze bieten WLAN an.
Europa	Schweden	m WLAN-Verzeichnis sind derzeit etwa 100 Hotspots in ganz Italien registriert, davon ca. 25% kostenlos.	WLAN-Zugang in öffentlichen Bibliotheken ist zeitlich beschränkt. In Schweden gibt es keine Störerhaftung. Deshalb wird der Datenverkehr der Nutzer von Freifunk-Netzen aus Deutschland gebündelt und in Schweden an das Internet angeschlossen.
Europa	Dänemark	Laut (*) sind ca. 600 Hotspots verfügbar, davon nur 5% kostenlos.	
Europa	Spanien	Laut (*) sind ca. 500 Hotspots verfügbar, davon ca. 15% kostenlos.	
Asien	Taiwan	Reisende, die in die taiwanesische Hauptstadt Taipeh kommen, können sich schon 30 Tage vor Ankunft für ein landesweites Netzwerk aus 5000 Hotspots registrieren – kostenlos.	
Asien	Nordkorea	Keine öffentlichen WLAN-Hotspots.	WLAN-Nutzung ist für Ausländer verboten. Nur Behörden und besonders privilegierte, linientreue Parteifunktionäre haben Erlaubnis zur Nutzung eines Internetzugangs.
Asien	China	In den größeren Städten findet man zunehmend westliche Cafés, oft auch die Café-Kette Starbucks oder chinesische Kopien der Marke. Und praktisch alle Cafés in China bieten ein öffentliches WLAN an, das kostenlos genutzt werden kann. Selbst einige Restaurants oder westliche Fastfood-Ketten China haben kostenlose und anonyme Wifi-Zugänge installiert.	

Kontinent	Land	Beschreibung	Besonderheiten
Nordamerika	USA	In USA ist eine sehr große Zahl von öffentlichen Hotspots verfügbar. Ein großer Teil hiervon ist kostenpflichtig (etwa 80 Prozent). Im Hotspotverzeichnis (*) werden mehr als 10.000 Hotspots gelistet. US-Präsident Barack Obama will 3,2 Milliarden Dollar investieren, um alle amerikanischen Schulen bis 2018 mit WLAN auszurüsten	
Nordamerika	Kanada	Wie in USA, so sind auch hier sehr viele Hotspots verfügbar (knapp 600 laut (*)), davon ca. 25% kostenlos.	
Australien		Etwa 25% der Hotspots sind kostenlos. (*) listet ca. 420 Hotspots insgesamt.	
Neuaseeland		Etwa 10% der Hotspots sind kostenlos. (*) listet ca. 60 Hotspots insgesamt.	

Tabelle 22 Kostenfreies öffentliches WLAN im Ausland