Karaboga, Murat; Eisele, Daniel; Grigorjew, Olga
Friedewald, Michael (Ed.)

Book

White Paper Privatheit in öffentlichen WLANs : Spannungsverhältnisse zwischen gesellschaftlicher Verantwortung, ökonomischen Interessen und rechtlichen Anforderungen

Reference: Karaboga, Murat/Eisele, Daniel et. al. (2017). White Paper Privatheit in öffentlichen WLANs : Spannungsverhältnisse zwischen gesellschaftlicher Verantwortung, ökonomischen Interessen und rechtlichen Anforderungen. 1. Auflage. Karlsruhe : Fraunhofer-Institut für System- und Innovationsforschung ISI.
urn:nbn:de:0011-n-4458463.

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

White Paper

PRIVATHEIT IN ÖFFENTLICHEN WLANs

Spannungsverhältnisse zwischen gesellschaftlicher Verantwortung, ökonomischen Interessen und rechtlichen Anforderungen

White Paper

PRIVATHEIT IN ÖFFENTLICHEN WLANs

Spannungsverhältnisse zwischen gesellschaftlicher Verantwortung, ökonomischen Interessen und rechtlichen Anforderungen

Redaktion:
Murat Karaboga[1]

Autorinnen und Autoren:
Daniel Eisele[7], Olga Grigorjew[2], Murat Karaboga[1], Tobias Matzner[3], Tina Morlok[4], Maxi Nebel[2], Carsten Ochs[5], Rasmus Robrahn[6], Christine Rzepka[4], Hervais Simo Fhom[7],

(1) Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe
(2) Universität Kassel, Institut für Wirtschaftsrecht
(3) Universität Tübingen, Internationales Zentrum für Ethik in den Wissenschaften (IZEW)
(4) Universität München, Institut für Wirtschaftsinformatik und Neue Medien (WIM)
(5) Universität Kassel, Fachgebiet Soziologische Theorie
(6) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Kiel
(7) Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt

Herausgeber:
Michael Friedewald, Regina Ammicht Quinn, Marit Hansen, Jessica Heesen, Thomas Hess, Jörn Lamla, Christian Matt, Alexander Roßnagel, Sabine Trepte, Michael Waidner

Inhalt

Zusammenfassung

Der Zugriff auf das Internet hat sich durch die Verbreitung mobiler Endgeräte im vergangenen Jahrzehnt von der stationären hin zur mobilen Nutzung verändert. Da Kapazitäts- und Geschwindigkeitsbeschränkungen der meisten Mobilfunktarife die Möglichkeiten der mobilen Internetnutzung allerdings stark einschränken, bieten immer mehr gewerbliche, aber auch kommunale Akteure (kostenfreie) öffentliche WLANs an, die eine komfortablere Internetverbindung versprechen. Im internationalen Vergleich befindet sich Deutschland im Hinblick auf die Verbreitung solcher öffentlicher WLANs allerdings immer noch auf den hinteren Plätzen. Als Hauptgrund gelten haftungsrechtliche Unsicherheiten. Dabei wird im gesellschaftlichen Diskurs oft ausgespart, dass die Verbreitung öffentlicher WLANS auch die Möglichkeiten erhöht hat, auf personenbezogene Daten der WLAN-Nutzenden und auch Nicht-Nutzenden zuzugreifen. Dies ist sowohl aus datenschutzrechtlicher als auch aus strafrechtlicher Sicht problematisch.

Das vorliegende White Paper zeigt, welche technischen Ausspäh- und Zugriffsmöglichkeiten auf personenbezogene oder -beziehbare Daten in drahtlosen lokalen Netzwerken, also Wireless Local Area Networks (WLANs), bestehen und welche Gefährdungen diese für die informationelle Selbstbestimmung und Privatheit der Nutzerinnen und Nutzer mit sich bringen, welche Rahmenbedingungen das Recht setzt und welche technischen Schutzmöglichkeiten existieren.

Sozio-technischer Hintergrund

Bei öffentlichen WLANs ist zwischen offenen und verschlüsselten WLANs zu unterscheiden: Bei offenen WLANS erfolgt die Nutzung ohne Anmeldung und damit anonym, Daten werden im Klartext, also unverschlüsselt, übertragen. Bei verschlüsselten WLANs ist es notwendig, sich durch die Eingabe des Netzwerkschlüssels im Netz anzumelden; die Kommunikation erfolgt dann in verschlüsselter Form. Anders als die Begrifflichkeit *öffentliches WLAN* suggerieren mag, ist allerdings noch unklar, wie die Verantwortlichkeiten im Hinblick auf Sicherheit und Privatheitsschutz bei den beteiligten Akteuren tatsächlich verteilt sind: Also wie viel Schutzverantwortung dem Staat, den Betreibern der WLAN-Zugänge oder den Nutzerinnen und Nutzern zukommt. Diese Fragen sind derzeit Gegenstand der öffentlichen Debatte um (kostenfreie) öffentliche WLAN-Zugänge. Allgemein akzeptierte und abschließende Antworten gibt es derzeit noch nicht. Sowohl für öffentliche als auch für gewerbliche Akteure stehen unterschiedliche Prioritäten im Vordergrund: Während bei Städten und anderen öffentlichen Betreibern die Grundversorgung der Bevölkerung mit einem Internetzugang im Vordergrund steht, verfolgen Unternehmen wirtschaftliche Interessen wie die Analyse des Kundenverhaltens, Steigerung der Kundenbindung, aber auch das Abschöpfen und Vermarkten von Nutzungsdaten. Für Nutzerinnen und Nutzer bestehen die Vorteile vor allem in der kostenfreien und komfortableren Nutzung des Internets.

Bedrohungs- und Überwachungspotenziale in öffentlichen WLANs

In öffentlichen WLANs existiert eine Vielzahl von Ausspäh- und Zugriffsmöglichkeiten auf personenbezogene oder -beziehbare Daten. Während sich passive Angreifer auf das Abhören und Abspeichern des Datenverkehrs im WLAN beschränken, können aktive Angreifer explizit in die Kommunikation eingreifen und die Integrität des Datenverkehrs kompromittieren. Das heißt, dass bei einem aktiven Angriff die gesendeten Nachrichten geändert, erweitert, umgeleitet, gelöscht, die Funk- bzw. Internetverbindung

unterbrochen oder gar fremde Inhalte (bspw. Malware) auf dem Gerät des Opfers ausgeführt werden können. Grundsätzlich können aktive Angreifer zwar größeren Schaden anrichten als passive Angreifer, in Bezug auf die Erstellung von Bewegungsprofilen und die Aufzeichnung des gesamten Datenverkehrs, der über den WLAN-Zugang läuft, stellen passive Angreifer – insbesondere WLAN-Betreiber, Internet Service Provider und Analysedienste – jedoch das größte Bedrohungspotenzial dar.

WLAN-Infrastrukturen werden häufig auch von einzelnen Gewerbetreibenden bereitgestellt und selbst verwaltet. Es gibt aber eine Vielzahl von Dienstleistern, die die Bereitstellung der Infrastruktur übernehmen und Gewerbetreibende zudem mit Analysen über ihre Kundschaft versorgen. Tracking und Profilbildung können zwar durchaus auch positive Auswirkungen haben und von den Nutzerinnen und Nutzern erwünscht sein, wenn ihnen beispielsweise auf Grundlage von Standortdaten und Bewegungsprofilen spezielle Angebote gemacht werden oder ein gesuchtes Produkt im Supermarkt schneller gefunden werden kann. Gleichzeitig birgt diese Art des meist intransparent praktizierten Kundentrackings auf Basis von WLAN-Signalen aber auch eine Reihe von Privatheitsrisiken: Der Zugriff der WLAN-Betreiber auf Konto- und Registrierungsdaten, gerätespezifische und ableitbare Daten sowie auf Nutzungs- und Verhaltensdaten kann sich negativ auf die informationelle Selbstbestimmung auswirken und etwa zum Verlust bzw. zu einer Einschränkung der Entscheidungsfreiheit führen, sehr weitgehende elektronische Überwachung ermöglichen und die Offenlegung sensibler oder vertraulicher Daten zur Folge haben. Auf diese Weise können Nutzerinnen und Nutzer bei ihrem Weg durch eine Stadt „auf Schritt und Tritt verfolgt", auch unbescholtene Demonstrationsteilnehmer identifiziert und selbst sensibelste Kommunikationsinhalte und Persönlichkeitsmerkmale offengelegt werden.

Haftungsrechtlicher Rahmen

Nach bisheriger Rechtslage muss jemand, der ein WLAN betreibt, dafür haften, wenn über dieses Netzwerk Rechtsverletzungen begangen werden. Im Hinblick auf die rechtliche Entwicklung der Störerhaftung beim offenen WLAN-Betrieb ist festzuhalten, dass alle WLAN-Anbieter – ob gewerblich oder privat – nach dem Telemediengesetz auch Access-Provider sind. Nach dem Urteil des Europäischen Gerichtshofs (EuGH) vom Mai 2016 können die (gewerblichen) WLAN-Anbieter auf gerichtliche oder behördliche Anordnung zur Verschlüsselung des WLAN-Zugangs und zur Nutzeridentifizierung verpflichtet werden. Allerdings besteht hierfür keine grundsätzliche Pflicht, es muss zunächst eine nachgewiesene Rechtsverletzung vorliegen. Zu Privatpersonen als Betreiber eines WLANs trifft der EuGH jedoch keine Aussage. Welche Auswirkungen das Urteil des EuGH auf die Praxis und auf das kürzlich novellierte Telemediengesetz haben wird, muss sich erst zeigen. Die deutsche Bundesregierung wollte die EuGH-Entscheidung, entgegen zahlreicher Expertenmeinungen, nicht abwarten. Stattdessen stützte sie sich bei der Gesetzesbegründung im November 2015 maßgeblich auf die Schlussanträge des EuGH-Generalanwalts, denen der EuGH im Hinblick auf die Frage nach der Nicht-Eignung von Verschlüsselung allerdings nicht gefolgt ist.

Mittlerweile hat die Bundesregierung den Nachbesserungsbedarf erkannt: Ende Februar 2017 hat das Bundeswirtschaftsministerium einen Referentenentwurf für ein Drittes Gesetz zur Änderung des Telemediengesetzes vorgelegt und dazu eine Verbändeanhörung eingeleitet. Mit dem Referentenentwurf sollen Nachbesserungen am Telemediengesetz im Hinblick auf das EuGH-Urteil vorgenommen werden, um Rechtssicherheit beim Betrieb offener WLAN-Netze zu schaffen. Dieser Prozess ist noch nicht abgeschlossen, so dass derzeit noch unklar ist, wann und in welcher Form eine Nachbesserung erfolgen wird.

Solange Unsicherheit bei den WLAN-Anbietern aufgrund der unklaren Rechtslage fortbesteht, werden auch weiterhin viele Organisationen, Gewerbetreibende und Privatpersonen ihre WLANs für die Öffentlichkeit nicht öffnen wollen.

Strafrechtlicher Rahmen

Trotz des Eingriffs in die informationelle Selbstbestimmung zahlreicher Betroffener und trotz vielfältiger Straftatbestände sind Angriffe auf offene WLANs durch das Strafgesetzbuch bislang nur unzureichend erfasst.

Bei der Verfolgung von strafrechtlich relevanten Angriffen existiert ein grundsätzlicher Zielkonflikt: Um Angreifer strafrechtlich zu belangen, müssten diese zudem identifiziert werden. Ein Rückgriff auf konkrete Täter ist jedoch nur möglich, wenn WLAN-Anbieter die Nutzung ihres WLANs protokollieren, indem Nutzerdaten erhoben und auf Vorrat gespeichert werden, um ggf. Straftäter zu identifizieren. Dies widerspricht jedoch nicht nur der Idee offener WLANs, sondern auch den geplanten Regelungen zur Störerhaftung des Telemediengesetzes, da dem Anbieter umfangreiche Pflichten auferlegt werden müssten, die die Neuregelung zur Störerhaftung gerade abzuschaffen versucht.

Datenschutzrechtlicher Rahmen

Betreiber öffentlicher WLANs müssen sich der Tatsache bewusst sein, dass ihre Tätigkeit unter die strengen Datenschutzvorschriften des Telekommunikationsrechts fällt. Nur weil ein Betreiber seiner Kundschaft einen WLAN-Zugang zur Verfügung stellt, bedeutet das noch nicht, dass man über die dabei anfallenden Daten frei verfügen kann. Vielmehr ist der Anbieter eines WLANs gerade wegen seiner weitreichenden Eingriffs- und Analysemöglichkeiten dazu verpflichtet, das Fernmeldegeheimnis zu wahren.

Auch wenn kein WLAN angeboten wird, sondern Kundenanalysen auf der Verfolgung WLAN-fähiger Geräte beruhen, gibt es hierfür im bisherigen Datenschutzrecht keine Rechtsgrundlage, auf die sich der jeweilige Betreiber berufen könnte. Wer eine solche Kundenanalyse in seinem Ladenlokal oder sonstigem Betrieb durchführen möchte, muss sich bewusst sein, dass er datenschutzrechtlich hierfür verantwortlich ist. Das gilt auch dann, wenn er die Analyse durch einen spezialisierten Anbieter solcher Dienste durchführen lässt. An dieser Rechtslage wird sich auch mit der Geltung der neuen Datenschutz-Grundverordnung (DSGVO) ab dem 25. Mai 2018 nichts ändern, deren Normen teilweise strikter formuliert sind, als die entsprechenden Normen im bisherigen Bundesdatenschutzgesetz.

Aus den Ergebnissen des White Papers lassen sich für unterschiedliche Zielgruppen Empfehlungen ableiten, um die Privatheit der Nutzenden in öffentlichen WLANs besser zu schützen.

Empfehlungen für Nutzerinnen und Nutzer[1]

- Das **Ausschalten des WLAN-Adapters** bringt den größtmöglichen Schutz vor den beschriebenen Überwachungsmöglichkeiten, **wird von uns allerdings nur eingeschränkt empfohlen**, da damit auch alle Vorzüge wegfallen, die öffentliche WLANs und damit eine stabilere und schnelle Internetverbindung mit sich bringen und die einen Kernaspekt der Nutzung WLAN-fähiger Endgeräte darstellen. Die Gewährleistung des Schutzes personenbezogener Daten mittels staatlich beaufsichtigter und durch Hersteller und Infrastrukturbetreiber eingesetzter technischer Schutzvorkehrungen muss auch dann gegeben sein, wenn das WLAN aktiviert bleibt.
- Die **Verwendung eines virtuellen privaten Netzwerks (VPN)** stellt grundsätzlich eine praktikable Selbstdatenschutzmöglichkeit dar. Mit einer VPN-Verbindung können Daten in einem ansonsten nicht vertrauenswürdigen Netz, also etwa einem öffentlichen WLAN, sicher übertragen werden. Sofern der VPN-Server nicht vom Nutzenden selbst betrieben wird, müssen die Nutzenden allerdings dem VPN-Anbieter vertrauen können.
- Die **Änderung des Nutzungsverhaltens** in öffentlichen WLANs ist eine weitere Selbstdatenschutzmöglichkeit: So sollten insbesondere über nicht vertrauenswürdige Netze keine vertraulichen Daten kommuniziert werden. Dazu zählt etwa die Anmeldung bei Online-Banking-Diensten, E-Mail-Konten und in sozialen Netzwerken.[2]
- Die **Nutzung einer UMTS- oder LTE-Verbindung** bei der Verwendung von anmeldepflichtigen Online-Diensten verspricht mehr Sicherheit als eine nicht vertrauenswürdige WLAN-Verbindung.
- Die **Deaktivierung der Datei- und Verzeichnisfreigaben** am Nutzergerät ist eine hilfreiche Möglichkeit, um zu verhindern, dass Fremde auf private Inhalte zugreifen können, die auf dem Gerät gespeichert sind.
- Die **Deaktivierung der automatischen Anmeldung mit bekannten Netzen** kann zu verbesserter Sicherheit beitragen, weil so die Wahrscheinlichkeit verringert wird, dass man sich mit einem gefälschten Zugangspunkt verbindet, der den Namen eines bekannten Netzwerks trägt. Einen wirklich wirksamen Schutz bietet diese Methode allerdings nicht: Denn selbst bei ausgeschalteter automatischer Anmeldung stellt sich die Frage, wie Nutzerinnen und Nutzer ein vertrauenswürdiges von einem nicht-vertrauenswürdigen Netz unterscheiden können.

Empfehlungen für Betreiber öffentlicher WLANs und Gerätehersteller

- Öffentliches WLAN sollte grundsätzlich nicht offen und damit unverschlüsselt sein, die Betreiber
    - sollten sich stets versichern, dass für die Erhebung, Speicherung oder Verarbeitung personenbezogener Daten **eine gesetzliche Erlaubnis besteht oder eine Einwilligung eingeholt wurde**, und,
    - dass **personenbezogene Daten nur insoweit erhoben, gespeichert und verarbeitet werden, wie es zur Bereitstellung des WLANs erforderlich**

ist. Auch wenn Betreiber aufgrund einer Einwilligung grundsätzlich dazu berechtigt sind, personenbezogene Daten zu erheben, **setzt das Datenschutzrecht bspw. Kundenanalysen auf der Grundlage der Verfolgung von WLAN-fähigen Geräten, enge Grenzen**.

- **WLAN-Anbieter sollten zum Zwecke der Zugangskontrolle auf WPA2-Enterprise zurückgreifen**. Dabei ist darauf zu achten, dass die Vertrauenswürdigkeit der darunterliegenden Public-Key-Infrastruktur, also einer vertrauenswürdigen Stelle, die für Authentizität des Nutzenden durch das Signieren eines digitalen Zertifikats bürgt, gewährleistet ist. Ferner ist die mit WPA2-Enterprise verbundene Passwortverwaltung unter Berücksichtigung der angemessenen Sicherheitsrichtlinien (z. B. BSI-Grundschutzkatalog[3], NIST-Richtlinien[4]) zu gestalten.

- **Landing pages (Einstiegsseiten) müssen so konfiguriert werden, dass sie nicht als Instrument einer versteckten Ausspähung und Überwachung dienen**:
  - Nutzenden von öffentlichen WLANs muss es möglich sein, Tracking-Cookies zu entfernen bzw. zu blockieren, ohne dass die Funktionalitäten der Einstiegsseite (u. a. Anmeldung bzw. Registrierung, Lesen der AGB etc.) beeinträchtigt werden; und
  - eine verständliche und nachvollziehbare Aufklärung in Hinblick auf IT-Sicherheit und Privatheit für Nutzende muss erfolgen. Insbesondere müssen Nutzende auf mögliche Risiken im System, sowie bestehende Sicherheitsvorkehrungen und weitere Tools (z. B. VPN), die selbstverantwortlich eingesetzt werden können, aufmerksam gemacht werden.
  - Darüber hinaus sollten Landing pages frei von sogenannten Social-Plugins (insbesondere Social-Media-Logins) betrieben werden.
- **MAC-Adressen, Passwörter und andere erfasste Daten müssen sicher aufbewahrt werden**. Im laufenden Betrieb erfassen öffentliche WLAN-Infrastrukturen und Dienste eine Vielzahl an teilweise sensiblen Daten, die der Betreiber durch Zugangs- und Zugriffsmechanismen hinreichend schützen muss.
- **Robuste und kontinuierliche Endpoint-Security**. Wichtige Netzwerkkomponenten wie Router und Switches können durch „Hintertüren" kompromittiert sein. Betreiber von WLAN-Infrastrukturen und betroffene Hardware-Hersteller müssen daher bei der Auswahl entsprechender IT-Komponenten sowie bei der Implementierung und dem Betrieb ihrer Systeme den Stand der Technik beachten. Zur Umsetzung dieser Ziele und damit zur nachhaltigen Erhöhung der Cyber-Sicherheit in der Gesamtinfrastruktur, mit der auch Viren- und Phishing-Angriffe erschwert werden können, gehören u. a. folgende Aspekte:
  - Routinemäßige und fundierte Bewertung des Sicherheitszustands der Netzwerkkomponenten und Absicherung wichtiger Endpunkte gemäß relevanter Sicherheitsleitfäden. Einen derartigen Leitfaden stellt beispielsweise das BSI in Form des IT-Grundschutz-Katalogs bereit.[5]
  - Ausschließlich Hardwarekomponenten einsetzen, die gemäß effektiver Sicherheitskriterien hergestellt worden sind. Kriterien für sichere Hardware definiert bspw. der Bundesverband IT-Sicherheit (Teletrust).[6]
- Die **Größe des WLAN-Funkbereichs sollte durch den WLAN-Betreiber begrenzt werden**. Eine Einschränkung der Reichweite des Funksignals beispielsweise auf das Geschäft kann das Risiko nicht autorisierter Netzzugriffe reduzieren, da Angreifer dann deutlich näher an den WLAN-Hotspot herantreten müssen und somit Angriffe aus sicherer Entfernung schwieriger durchzuführen sind.

Empfehlungen für Forschung und Entwicklung

Die vorgestellten Schutzmaßnahmen bieten keinen vollumfänglichen Privatheitsschutz. Daher wird prioritärer Forschungs- und Entwicklungsbedarf im Hinblick auf neuartige Mechanismen und Techniken zum Schutz von Anonymität und Privatheit im Kontext neu entstehender WLAN-Infrastrukturen und -Dienste gesehen. Forschungsbedarf besteht vor allem in den folgenden Themenfeldern:

- **Metriken und Verfahren zur holistischen Vertrauensbewertung in WLAN-basierten Infrastrukturen und Diensten**:
  - Entwicklung und Bewertung holistischer Ansätze für die Nutzerinnen und Nutzer WLAN-fähiger Endgeräte zur automatisierten Erkennung kompromittierter bzw. bösartiger öffentlicher WLAN-Zugangspunkte.
  - Identifizierung von praxisrelevanten Metriken zur Bewertung von WLAN-basierten Infrastrukturen und Diensten im Hinblick auf die Einhaltung datenschutzrechtlicher Anforderungen und Privatheitserwartungen.
  - Darauf aufbauend: Entwicklung und Bewertung neuer effektiver Selbstdatenschutztechniken. Insbesondere soll Verbraucherinnen und Verbrauchern die Möglichkeit gegeben werden, die Vertrauenswürdigkeit von WLAN-Infrastrukturen und -Diensten zu messen und deren Nutzung entsprechend zu steuern bzw. einzuschränken.
- **Sichere, benutzerfreundliche und datenminimierende Authentifikation und WLAN-Nutzung[7] auf Basis des neuen Personalausweises (nPA)**:
  - Weiterentwicklung von gegenwärtigen kryptographischen Systemen und Protokollfamilien zur datenminimierenden Authentifizierung. Es muss erforscht werden, inwieweit eine effektive und skalierbare Privatheit, benutzerfreundliche Authentifizierung im Kontext neu entstehender WLAN-Angebote zu gewährleisten ist, ohne das Nutzenpotenzial solcher Angebote zu beeinträchtigen. Denkbar wären Ansätze, die den nPA als Vertrauensquelle im Sinne des kürzlich vom Bundesinnenministeriums vorgelegten „Cyber-Sicherheitsstrategie für Deutschland 2016“[8] integrieren. Bestehende, eingeschränkte Mechanismen und Verfahren des nPA, wie etwa Pseudonyme und die selektive Preisgabe von Identitätsattributen, müssen weiterentwickelt werden. So könnten WLAN-Betreibern dann vergleichbar sichere und leicht integrierbare Identitätsmanagement-Lösungen bereitgestellt werden, die aber eine Identifizierung und Verkettung der Nutzeraktivitäten technisch nur bedingt – z. B. im Falle einer gesetzeswidrigen Nutzung – möglich machen.
  - Darüber hinaus sollten Techniken erforscht werden, die eine Verlagerung wichtiger Funktionen des nPA (z. B. Online-Ausweisfunktion und die Signaturfunktion) auf das mobile Gerät ermöglichen, für die derzeit ein zusätzliches Chipkarten-Lesegerät benötigt wird. Durch den Verzicht auf zusätzliche Hardware und durch die Gewährleistung vergleichbar hoher Sicherheitsgarantien können die angestrebten technischen Lösungen zur Überwindung von Nutzungsbarrieren beitragen.
- **Schließlich besteht weiterer dringender Forschungs- und Entwicklungsbedarf im Hinblick auf Mobile Location Analytics.**[9]

Empfehlungen für Politik, Gesetzgebung und Datenschutzbehörden

- **Die Zertifizierung von WLAN-Anbietern** muss mittels staatlicher Unterstützung vorangetrieben werden. Die Zertifizierung könnte u. a. bei öffentlichen Ausschreibungen ein wichtiges Auswahlkriterium sein.
- **Alle Router und Switches in öffentlichen WLANs sind als sicherheitskritische Komponenten zu betrachten.** Sie müssen einen hohen Sicherheitsstandard erfüllen und bspw. nach Common Criteria EAL4+ zertifiziert sein.[10]
- **Beseitigung der Rechtsunsicherheit aus haftungsrechtlicher Sicht**: Die auch nach dem EuGH-Urteil anhaltende Rechtsunsicherheit muss durch den nationalen Gesetzgeber beseitigt werden. Eine gesetzliche Klarstellung im Telemediengesetz ist unter Beachtung der determinierenden Rechtspositionen erforderlich.
- **Anpassungen des Strafrechts**. Juristische Regelungen müssen einen Ausgleich zwischen dem Interesse der Allgemeinheit an offenen WLANs und deren Anbietern an einem rechtssicheren Betrieb dieser Netzwerke einerseits und dem Strafverfolgungsanspruch bei Verstoß gegen strafrechtliche Normen andererseits finden. Deshalb ist eine Konkretisierung der Regelungen zu den entsprechenden Straftatbeständen notwendig, damit eine Strafverfolgung überhaupt möglich wird.
- **Art. 8 Abs. 2 des Entwurfs der e-Privacy-Verordnung sollte nicht bestehen bleiben**. Ein Hinweis der WLAN-Betreiber, dass Mobile Location Analytics bzw. Offline-Tracking durchgeführt wird, ist nicht geeignet, dieses zu legitimieren. Stattdessen ist zu überlegen, ob diese Methoden des Trackings zumindest dann zu verbieten sind, wenn dabei personenbezogene Daten verarbeitet werden.

1 Einleitung

Das Konzept des Desktop-PCs wirkt - mit Blick auf die zunehmend mobile Nutzung des Internets - geradezu anachronistisch. Viele Nutzerinnen und Nutzer[11] greifen mittlerweile überwiegend auf Smartphones oder Tablets zurück, um im Internet zu agieren, und erwarten zeitlich und räumlich umfassenden Zugriff und Erreichbarkeit: Daten und Kommunikationspartner sollen möglichst immer und von überall aus zu erreichen sein. Doch nicht nur unsere Kommunikation ist 'mobil' geworden, auch alltägliche Aufgaben wie Einkaufen, Zeitung lesen und Banküberweisungen werden zunehmend über die Nutzung von Apps, also außerhalb der eigenen vier Wände erledigt. Bild-, Dokument-, Video- und andere Dateien landen dabei, anders als in der Vergangenheit, nicht mehr auf einer Festplatte, sondern werden von einer Vielzahl von Geräten fast automatisch und zu den unterschiedlichsten Zwecken in „die Cloud" hochgeladen. Zuhause gestaltet sich dies dank DSL oder Kabelanschluss zumeist problemlos, jedoch gilt dies unterwegs nicht mehr unbedingt: Zwar bieten die meisten Telekommunikationsanbieter mittlerweile mittels LTE auch unterwegs Bandbreiten von über 100 MBit/s an, was dem klassischen Anschluss zuhause gleichkommt, jedoch meistens nur mit eingeschränktem Datenvolumen. Kapazitäten von weniger als 1 GB Volumen pro Monat reichen oftmals nicht aus, um den beschriebenen Nutzungsstil zu pflegen. Nach Erreichen des Limits wird die Verbindungsgeschwindigkeit von Seiten der Telekommunikationsanbieter dann zumeist auf etwa 56kbit/s gedrosselt, was der Internetverbindung mit einem Modem Mitte der 1990er Jahre gleicht.

Solcherlei Kapazitätsbeschränkungen schlagen allerdings dort, wo zunehmend öffentliche Drahtlosnetzwerke bzw. Wireless Local Area Networks (WLANs) angeboten werden, immer weniger zu Buche. Kommerzielle Anbieter, von den Betreibern kleiner Geschäfte, Cafés oder Restaurants über Kaufhäuser bis zu Shopping Malls bieten Kunden und Passanten aus verschiedensten Gründen die Möglichkeit, das Internet zu nutzen, ohne dabei die mobilen Nutzungslimits zu strapazieren. Stadtverwaltungen vernetzen derweil öffentliche Plätze und andere zentrale Orte, wie etwa Bahnhöfe und Marktplätze, um die Attraktivität von Städten zu erhöhen. Auf diese Weise können bspw. sowohl sozial benachteiligte Gruppen (etwa von Armut betroffene Menschen oder Geflüchtete) als auch Touristen auf das Internet zugreifen, die sonst nur über einen sehr eingeschränkten, sehr teuren oder gar keinen Internetzugriff verfügen würden. Auch andere nichtkommerzielle Anbieter unterstützen die Versorgung der Bevölkerung mit Internet: Beispielsweise versucht die in vielen deutschen Städten aktive Initiative *Freifunk* zusammen mit den Anwohner(inne)n ein vollkommen freies und für alle offenes WLAN anzubieten. Unabhängig davon, wer das WLAN bereitstellt, ist es für die Nutzenden oftmals eine sehr willkommene Möglichkeit, das knapp bemessene mobile Datenvolumen zu schonen. Zudem sind die Hürden, die überwunden werden müssen, um öffentliches WLAN in Anspruch zu nehmen, eher niedrig. Entweder erweist sich das genutzte WLAN als komplett unverschlüsselt, dann reicht ein einfacher Klick auf den Namen des Netzwerkes um sich zu verbinden; oder ein relativ triviales Passwort findet Verwendung, welches man einfach bei der das WLAN-betreibenden Institution erfragen, von großen Tafeln abschreiben kann o. ä.

Zwar sind WLAN-fähige Endgeräte in Deutschland weit verbreitet und die Internetnutzung gleichbleibend hoch, doch in Bezug auf die Verbreitung öffentlicher WLANs befindet sich Deutschland im internationalen Vergleich auf den hintersten Plätzen.

So entfallen auf jeden deutschen Bundesbürger etwa drei WLAN-fähige Endgeräte, womit die Bundesrepublik dem weltweiten Durchschnitt (1,2 Geräte pro Kopf) deutlich voraus ist. Und mit einer regelmäßigen Internetnutzung von über 80% aller in Deutschland lebenden Personen befindet sich die Bundesrepublik immerhin noch im europäischen Durchschnitt.[12] Blickt man allerdings auf die Verbreitung öffentlicher WLAN-

Zugänge, ergibt sich ein gänzlich anderes Bild. So gehört die Nutzung öffentlicher WLANs in vielen Staaten zum Alltag. Aktuelle Zahlen des Bitkom e. V., des eco Verbandes der deutschen Internetwirtschaft und Marktstudien von NinthDecimal zeigen, dass in den letzten Jahren die Anzahl öffentlicher WLANs bzw. WLAN-Hotspots weltweit stark angestiegen ist. Während es 2006 weltweit nur 132.000 öffentliche Zugangspunkte gab, konnte man 2011 bereits auf etwa 683.000 Hotspots weltweit zugreifen.[13] Die höchste WLAN-Dichte hatte im Jahr 2011 Großbritannien mit 234 Hotspots pro 100.000 Einwohner. Auf den Plätzen zwei und drei folgten Japan und Südkorea mit 98 bzw. 88 Hotspots pro 100.000 Einwohner.[14] Aktuellere Zahlen aus dem Jahr 2014 zeigen, dass Großbritannien mit nun 287 Hotspots pro 100.000 Einwohner seine Hotspotdichte zwar weiter steigern konnte, Südkorea allerdings das Hotspotangebot seither deutlich stärker ausgebaut hat und nun mit 374 Hotspots das Land mit der höchsten WLAN-Dichte darstellt.[15] Während andere Länder auf diese Weise bereits eine nahezu flächendeckende Nutzung öffentlicher WLANs ermöglicht haben, ist die Abdeckung in Deutschland vergleichsweise gering. So gab es im Jahr 2014 deutschlandweit lediglich 19 Hotspots pro 100.000 Einwohner.[16] Ein Großteil davon sind wiederum private, (teil-)öffentliche Hotspots unter Kontrolle der großen Netzbetreiber, gefolgt von Hotspots mit Sicherung ohne individuelle Authentifizierung, wie z. B. in Restaurants oder Cafés.[17]

Als Ursache für den geringen Ausbau öffentlicher WLANs wird insbesondere die rechtliche Situation ausgemacht.[18] Öffneten die Inhaber ihre WLANs für die Öffentlichkeit, befürchteten sie, nach der bisher in Deutschland herrschenden Rechtslage im Zweifelsfall für Rechtsverletzungen der Nutzenden zu haften, wenn diese von ihrem Anschluss aus begangen wurden (sog. Störerhaftung). Hatten sich die WLAN-Anbieter nach den Grundsätzen der Störerhaftung für das Vergehen der Nutzenden zu verantworten, konnten sie zum einen auf Unterlassung in Anspruch genommen werden. Zum anderen waren die WLAN-Anbieter auch einem Abmahnrisiko ausgesetzt.[19]

Schließlich entwickelte sich die Störerhaftung beim WLAN-Betrieb in den vergangenen Jahren zu einem profitablen Geschäftsmodell, das von Anwaltskanzleien im Auftrag der Rechteinhaber bzw. ihrer Vertreter forciert wurde: Entweder zahlte der abgemahnte WLAN-Anbieter widerspruchslos oder er unterlag vor Gericht. Im letzteren Fall hat ein WLAN-Anbieter zudem sowohl für die gerichtlichen als auch außergerichtlichen Kosten aufzukommen, die nicht selten im vierstelligen Bereich liegen.[20] Schätzungsweise 150.000 Filesharing-Abmahnungen mit einer Forderungshöhe von durchschnittlich 500 bis 1000 € werden in Deutschland jährlich verschickt.[21]

Das Risiko, abgemahnt zu werden war insofern besonders problematisch, weil die Störerhaftung beim Betrieb offener WLANs gesetzlich nicht geregelt war und von den deutschen Gerichten sehr uneinheitlich bewertet wurde. Potentielle WLAN-Anbieter waren angesichts der herrschenden Rechtsunsicherheit und des Abmahnrisikos verunsichert und verzichteten infolgedessen auf die Bereitstellung öffentlicher, aber insbesondere auch offener WLAN-Zugänge. Um dem entgegenzuwirken, erfolgte im Zuge der Novellierung des Telemediengesetzes im Juli 2016 eine rechtliche Regelung der Störerhaftung beim Betrieb öffentlicher WLANs. Diese zielt unter anderem darauf, zum Ausbau öffentlicher WLANs und zu mehr Rechtssicherheit bei den WLAN-Anbietern beizutragen.[22] Auch der Europäische Gerichtshof (EuGH) hat sich mit den haftungsrechtlichen Fragen der Störerhaftung befasst und im September 2016 seine Entscheidung verkündet. Diese kollidiert jedoch zum Teil mit der Regelung der Störerhaftung im TMG (§ 8 Abs. 3) und stellt die WLAN-Anbieter vor neue haftungsrechtliche Probleme.

Auf der anderen Seite – aber sehr viel weniger beachtet – bieten öffentliche WLAN-Infrastrukturen in vielen Fällen auch Einfallstore für Praktiken, die straf- und datenschutzrechtlich bedenklich sind. Bei öffentlichen WLANs kann dies einerseits – aus strafrechtlicher Perspektive – Angreifer betreffen, die durch zahlreiche Ausspähmöglichkeiten Zugriff auf Nutzerendgeräte erhalten können. Andererseits – aus datenschutzrechtlicher Perspektive – aber auch private, gewerbliche und kommunale Anbie-

ter öffentlicher WLANs betreffen, die jeweils aus ihrem eigenen Partikularinteresse heraus eine weitergehende Nutzung der Daten von Bürger(inne)n bezwecken, die bei der Nutzung – teilweise allerdings auch bei Nichtnutzung – öffentlicher WLANs anfallen.

WLANs werden damit in zunehmendem Maße Teil des öffentlichen Raums. Angetrieben wird diese Entwicklung sowohl von rechtlichen Anforderungen als auch von öffentlichen Allgemeinwohl- sowie privatökonomischen Profitinteressen. Die dabei zu Tage tretenden Konflikte genau wie die vergleichsweise neuartige Weise, das Internet in die im öffentlichen Raum vollzogenen Alltagspraktiken zu integrieren, werfen gleichzeitig eine Reihe privatheitsrelevanter Fragen und Probleme auf: Worum handelt es sich genau bei öffentlichem WLAN und wie funktioniert die WLAN-Kommunikation? In welchem gesellschaftlichen Rahmen findet sie statt, und welche Akteursinteressen stehen dabei gegeneinander (Abschnitt 2)? Welches Bedrohungspotenzial lässt sich ausmachen, und zwar sowohl hinsichtlich krimineller Datendiebe als auch in Bezug auf privatheitsgefährdende datenökonomische Überwachungspraktiken (Abschnitt 3)? Wie sieht der regulatorische Rahmen genau aus, d. h. in welcher regulatorischen Tradition ist die Rechtsprechung zu freien WLANs zu verorten, und welcher haftungs-, straf- und datenschutzrechtliche Gesetzeskorpus wird wirksam (Abschnitt 4)? Welche technischen Gegenmaßnahmen existieren schließlich, um die bestehenden Risiken zu beseitigen oder zumindest abzuschwächen (Abschnitt 5)?

Das vorliegende White Paper leistet einen Beitrag zur Aufklärung des technischen, sozialen, ökonomischen und regulatorischen Status Quo öffentlicher WLANs, und mündet, basierend auf einer Zusammenschau all dieser Aspekte, in eine ethisch fundierte Gesamtbetrachtung dieser immer wichtiger werdenden soziotechnischen Infrastruktur des Alltags (Abschnitt 6).

2
Sozio-technischer Hintergrund

2.1 Definitionen

2.1.1 Infrastruktur

WLAN

WLAN steht für *Wireless Local Area Network* und bezeichnet ein drahtloses lokales Netzwerk bzw. ein lokales Funknetzwerk. WLANs werden typischerweise gemäß IEEE 802.11 – einem technischen und international etablierten Standard des Institute of Electrical and Electronics Engineers (IEEE) für die Kommunikation in Funknetzwerken aus dem Jahr 1997 – betrieben.[23] WLAN als Technik für drahtlose Datenübertragung zielt auf eine erhöhte Mobilität und einen verbesserten Komfort bei der Nutzung von vernetzten Kommunikationsendgeräten. Allerdings ist eine WLAN-basierte Datenübertragung per se langsamer und störanfälliger als vergleichbare Datenübertragung in kabelgebundene Local Area Networks (LANs). Die Reichweite in einem WLAN beschränkt sich in Gebäuden typischerweise auf einige Meter (im Außenbereich kann die Reichweite deutlich darüber liegen) und die Übertragungsgeschwindigkeit ist oft niedrig, da sich alle Nutzenden (im Folgenden auch bezeichnet als *WLAN-Clients*) die verfügbare Bandbreite teilen müssen. Neben gewissen Einschränkungen bzgl. der Reichweite und Übertragungsgeschwindigkeit besteht beim Einsatz von WLANs ein wesentliches Problem in der Anfälligkeit der Datenübertragung für Störungen. Derartige Störungen können entweder aufgrund umweltbedingter Einflüsse (z. B. Schnee-Sturm, starker Regen oder auch funkende Haushaltsgeräte) oder durch Dritte (z. B. Angreifer, die aus der Distanz die Vertraulichkeit der übermittelten Daten verletzen können) entstehen.

Öffentliches WLAN

Ein öffentliches WLAN bzw. öffentlicher WLAN-Hotspot ist ein Netz, das für die Öffentlichkeit bzw. für eine öffentliche Nutzung eingerichtet ist. Hierfür werden drahtlose Zugangspunkte, sog. WLAN access points (WLAN-APs) in öffentlichen Räumen installiert, mithilfe derer ein Internetzugang möglich ist. Die Begriffe „Öffentlichkeit" und „öffentlich" verweisen in diesem Zusammenhang darauf, dass die Nutzung des fraglichen WLAN jedenfalls im Prinzip einem unbestimmten Personenkreis, im Grunde also jedweder Person, offensteht. Hierunter fallen zum Beispiel WLAN-Angebote an öffentlichen Plätzen (u. a. Flughäfen, Bahnhöfe, Kaufhäuser, Cafés oder Hotels). Diese Netze können gebührenfrei oder gebührenpflichtig angeboten werden. Während öffentliche WLANs im Ausland oft als offene WLANs angeboten werden, ist dies in Deutschland aufgrund der herrschenden Gesetzeslage nicht der Fall (s. dazu Abschnitt 4). Damit ein WLAN-Anbieter im Falle einer Rechtsverletzung nicht selbst haften muss und die Ermittlung des Täters vereinfacht bzw. ermöglicht wird, ist daher häufig eine Identifizierung der Nutzenden erforderlich, bevor ein öffentliches WLAN genutzt werden kann. Zur Gewährleistung der Identifizierung wiederum werden die Nutzenden auf der Einstiegsseite[24] (englisch *landing page*) zum öffentlichen WLAN oder an der Cafétheke etc. zumeist dazu aufgefordert, sich mit Namen und E-Mail-Adresse zu registrieren.[25]

Offenes WLAN

Unter einem offenen WLAN wird ein Netz verstanden, mit dem sich Nutzende in Funkreichweite ohne Eingabe eines Passworts bzw. Zugangscodes verbinden können. Das sind demnach alle WLANs, die nicht durch eine Sicherheitsmethode gesichert sind. Ein

offenes WLAN kann sowohl von öffentlichen Stellen als auch von gewerblichen und nicht-gewerblichen Akteuren bereitgestellt werden.

Privates WLAN

Ein privates WLAN bezeichnet ein lokales Funknetz, welches von einer Privatperson bzw. einem Haushalt betrieben wird.[26] Der Zugang zu einem privaten WLAN ist typischerweise durch Zugangspasswörter und andere Sicherheitsfeatures im Heimrouter abgesichert. Zugangspasswörter und Sicherheitseinstellungen sollten idealerweise nur Personen im Haushalt bekannt sein. Passwörter sind allerdings häufig auch Freunden und Familienangehörigen, die bspw. zu Besuch sind, bekannt.

Freies WLAN

Freies WLAN bezeichnet ein offenes und vollständig gebührenfreies WLAN, das nicht von gewerblichen Anbietern, sondern von Privatpersonen, Vereinen usw. bereitgestellt wird.

2.1.2 Verwendung der Begrifflichkeiten

Grundsätzlich ist im vorliegenden White Paper von öffentlichen WLANs die Rede, weil darunter sowohl jene WLANs verstanden werden, die offen betrieben werde, als auch solche, deren Benutzung nur für einen ausgewählten Personenkreis vorgesehen ist. Je nach Abschnitt kann die Begrifflichkeit allerdings variieren. So setzen sich die technischen Abschnitte des White Papers (Abschnitte 2.2, 3 und 5) zwar mit dem Phänomen öffentlicher WLANs auseinander, doch betreffen einige Aussagen alle Arten von WLANs (also sowohl öffentliche als auch private WLANs), sodass in diesen Fällen ganz allgemein von WLANs, in anderen Situationen wiederum spezifisch von offenen WLANs gesprochen wird. Dagegen geht es bei den haftungs- und strafrechtlichen Fragestellungen in Abschnitt 4.2 und 4.3 insbesondere um den Betrieb unverschlüsselter, also offener WLANs, sodass in diesen Abschnitten entsprechend von offenen WLANs die Rede ist. In allen anderen Abschnitten wird darauf geachtet, dass situationsspezifisch der korrekte Begriff verwendet wird.

2.2 Funktionsweise der WLAN-Kommunikation und öffentlicher Hotspots

In diesem Abschnitt werden der Aufbau und die Funktionsweise von WLANs erläutert. Insbesondere werden die unterschiedlichen Betriebsarten eines WLANs näher dargestellt. Zuerst werden die Betriebsarten beschrieben, wie ein WLAN nach dem IEEE 802.11 Standard aufgebaut werden kann. Anschließend wird auf den, bei öffentlichen WLANs in der Regel verwendeten, sog. Infrastruktur-Modus näher eingegangen sowie der Kommunikationsverlauf dargestellt.

2.2.1 Betriebsarten

Die Art und Weise, wie WLAN-Hotspots betrieben werden, wird fast ausschließlich durch IEEE 802.11[27] definiert. IEEE 802.11 stellt im Grunde eine Familie von Richtlinien und Protokollen dar, die zum Zweck der Operabilität in fast allen Netzwerkroutern und Mobilendgeräten eingesetzt werden. Nach den IEEE 802.11-Normen können WLANs auf zwei Arten betrieben werden: Entweder im Ad-hoc- oder im Infrastruktur-Modus.

Ad-hoc-Modus

In dem so genannten Ad-hoc-Modus sind alle Stationen (STA) bzw. Endgeräte gleichberechtigt, es gibt keine zentrale Einheit, die den Zugang und die Kommunikation steuert (vgl. Abb. 01). Hier können zwei oder mehrere STAs direkt miteinander kommunizieren, sobald sie sich in unmittelbarer Funkreichweite voneinander befinden. Die Funkreichweite im Ad-hoc-Modus beträgt bis zu 100 Meter. Der Ad-Hoc-Modus ist geeignet, wenn eine kleine Anzahl an Endgeräten – ähnlich wie über Bluetooth – schnell Daten miteinander austauschen wollen und/oder sollen.

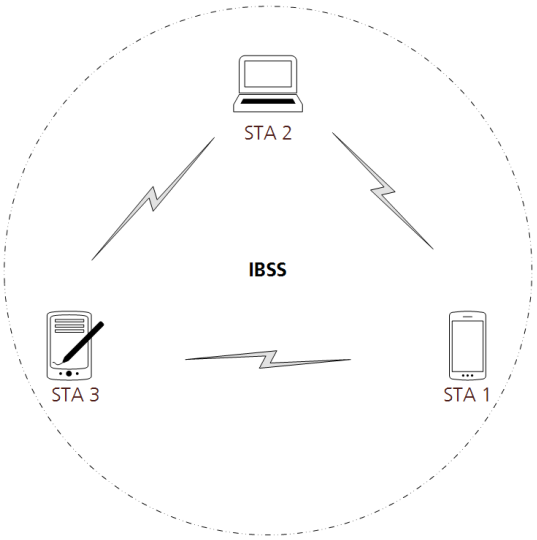

Abb. 01 Im Ad-hoc-Modus betriebenes WLAN

Infrastruktur-Modus

Der am weitesten verbreitete Betriebsmodus für WLAN-Kommunikation ist dagegen der Infrastruktur-Modus (siehe Abb. 02). Das liegt vor allem daran, dass WLANs fast ausschließlich für den Internetzugang – und nicht wie beim Ad-hoc-Modus zum Datenaustausch innerhalb der Funkreichweite – genutzt werden und die Besonderheiten des Infrastruktur-Modus diesen Anforderungen eher gerecht werden.

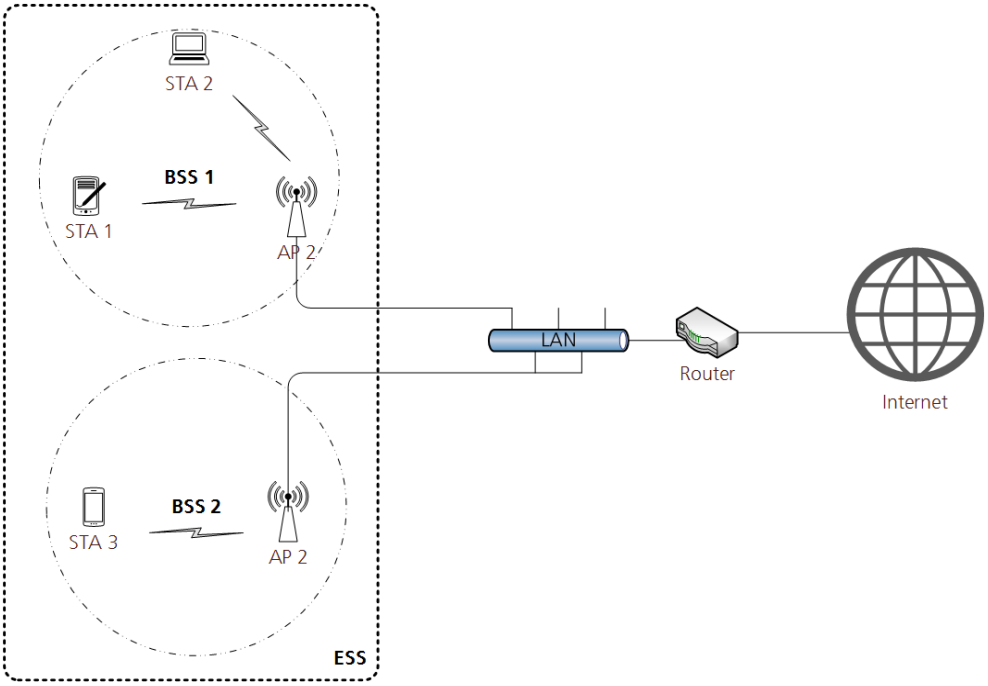

Abb. 02 Im Infrastruktur-Modus betriebenes WLAN

Im Infrastruktur-Modus findet die Kommunikation ausschließlich über eine zentrale Vermittlungsstelle oder über (WLAN-)Zugangspunkte bzw. -APs, statt. Ein oder mehre-

re Endgeräte bzw. STAs verbinden sich mit einem AP, wodurch sie ein Basic Service Set (BSS) bilden. Im Gegensatz zum Ad-hoc-Modus findet im Infrastruktur-Modus daher keine direkte Datenübertragung zwischen den einzelnen Endgeräten statt. Der AP übernimmt die Koordinierung des Datenverkehrs zwischen allen mit dem WLAN verbundenen Endgeräten. Als Vermittlungsstelle bietet der AP zudem eine Schnittstelle zum LAN.

Über die LAN-Schnittstelle kann der AP an einen Router angeschlossen werden, wodurch sich schließlich die Verbindung ins Internet ergibt. In heutigen Heimroutern ist in der Regel ein AP mit eingebaut, wodurch diese ehemals getrennt voneinander operierenden Systeme nunmehr als eine Einheit wahrgenommen werden. Im Gegensatz hierzu operieren in Firmennetzwerken und professionellen WLAN-Netzen[28] der AP und Router als getrennte Einheiten. Wenn mehrere APs miteinander verbunden werden, ergibt sich ein Funknetzwerk (sog. Distribution System (DS) bzw. Wireless Distribution System (WDS)). Verschiedene BSS, die über ein DS bzw. WDS verbunden sind, bilden ein Extended Service Set (ESS) welches wiederum als ein logisches Netzwerk betrachtet wird.

(Öffentliche) WLANs werden in der Regel im Infrastruktur-Modus betrieben. Darum wird im Folgenden ausschließlich dieser Modus näher betrachtet.

2.2.2 Kommunikationsaufbau im Infrastruktur-Modus

Um über ein WLAN ins Internet zu gelangen, müssen sich Nutzende bzw. deren Endgeräte zunächst mit einem AP verbinden, sich dort ggf. mittels Eingabe eines Nutzernamens und dazugehörigen Passworts authentifizieren, und bekommen anschließend vom AP eine Netzwerkadresse zugewiesen.

Verbindungsaufbau mit einem AP

In WLANs wird der Aufbau der Verbindung zwischen AP und Mobilendgeräten über das sogenannte Service Discovery Protocol (SDP) abgewickelt. Konkret sollen mithilfe des Protokolls AP und Endgeräte in die Lage versetzt werden, sich ihre Anwesenheit gegenseitig zu signalisieren sowie Details über Dienste der jeweiligen Gegenstelle auszutauschen. Im IEEE 802.11-Standard sind zwei Mechanismen hierfür vorgesehen: Ein passiver und ein aktiver Discovery-Mechanismus.

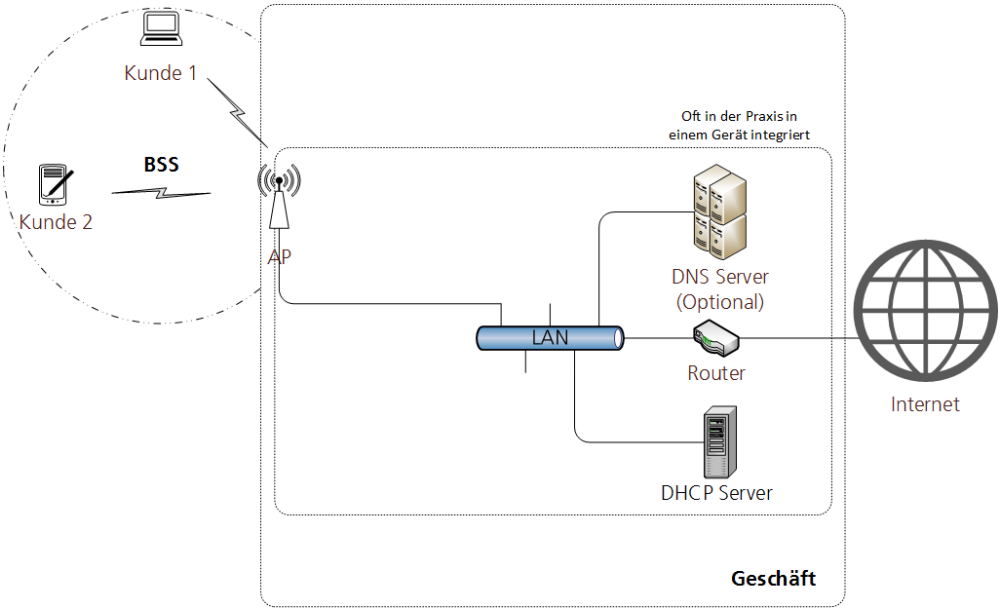

Abb. 03 Vereinfachter Aufbau eines öffentlichen WLANs, bei dem die Authentifizierung durch den AP erfolgt

Passiver Discovery-Mechanismus

In einem passiven Verbindungaufbau signalisiert der AP seine Anwesenheit durch das Aussenden[29] von sog. *Signal-Frames* (beacon management frames) an alle Geräte im Empfangsbereich. Signal-Frames sind Netzwerkpakete, die in regelmäßigen Abständen, etwa alle 100 Millisekunden, ausgesendet werden. Als Management-Pakete beinhalten sie Identifikations- und Netzwerkkonfigurationsparameter, an denen sich mobile Endgeräte orientieren können. Zu den Konfigurationsparametern gehören u. a. Details zu möglichen Übertragungsraten und unterstützten Verschlüsselungsverfahren. Für die Identifikation eines AP werden i. d. R. zwei Parameter verwendet: Der *basic service set identifier* (BSSID) und der Netzwerkname bzw. *service set identifier* (SSID). Die BSSID ist der eindeutige Geräte-Identifier, also die MAC-Adresse (*Medium Access Control*-Adresse)[30] des APs. Da MAC-Adressen in der Regel einzigartig sind, können darüber Geräte – in diesem Fall das BSS - eindeutig bezeichnet bzw. identifiziert werden (siehe auch Abschnitt 5.1.3). Die SSID wiederum kann als Klartextname des WLANs vom AP-Betreiber frei gewählt werden (z. B. Telekom-HotSpot oder Backstube Kamps-HotSpot). Das Zeitintervall, das die Häufigkeit bestimmt, mit der ein Signal-Frame gesendet wird – auch Beacon-Intervall genannt – ist im AP konfigurierbar. Definiert der Betreiber das Beacon-Intervall zu groß, kann der AP seine Anwesenheit nur selten signalisieren. Als Folge dessen bleibt das WLAN für viele Nutzerendgeräte je nach Intervall zunächst unsichtbar bzw. nur verzögert wahrnehmbar. Des Weiteren kann in einem Bedrohungsszenario, in dem ein Angreifer-WLAN als ein vertrauenswürdiges WLAN ausgegeben wird, ein langes Beacon-Intervall es Angreifern erleichtern, die Internet-Aktivitäten der Nutzenden abzugreifen. Dabei wird von Seiten der Angreifer ein eigenes WLAN betrieben, das dieselbe SSID erhält, wie jenes WLAN, das von den Nutzerinnen und Nutzern genutzt wird (z. B. den WLAN-Namen eines Cafés oder Kaufhauses). Indem das Beacon-Intervall des Angreifer-WLANs besonders niedrig angesetzt wird, wird dieses Netz Nutzerinnen und Nutzern schneller und häufiger angezeigt, die sich aufgrund dessen eher mit dem Angreifer-WLAN verbinden.

Aktiver Discovery-Mechanismus

Das Nutzerendgerät kann auch proaktiv die Anwesenheit eines WLAN-APs feststellen. Dafür sendet es einen sog. Probe Request an alle in Reichweite befindlichen WLAN-APs. Diese signalisieren ihre Präsenz wiederum durch ein Antwortsignal. Ein Probe Request beinhaltet Angaben über die eindeutige Identität (z. B. die MAC-Adresse) und technische Fähigkeiten (z. B. die Unterstützung des 802.11-Standards) des Nutzerendgerätes, sowie ggf. Angaben über die SSID möglicher WLAN-APs. Damit fragt das Endgerät alle Netzwerke ab, die es bereits kennt, indem es die Namen dieser Netzwerke über Probe Requests nach außen hin kommuniziert. Die SSIDs kennt das Nutzerendgerät von früheren Verbindungen mit den jeweiligen WLANs. Da es möglich ist, dass jene aus den vergangenen Interaktionen bekannten APs nicht in der Nähe des Nutzerendgeräts sind, beinhalten Probe Responses – Antworten von den APs – stets Angaben über die jeweilige SSID und alle für eine Authentifizierung und Verschlüsselung notwendigen Informationen der Kommunikation mit dem AP. Hinter dieser Methode steckt ein Effizienzgedanke: Hier können WLAN-Adapter in Nutzerendgeräten viel schneller nach einem oder nach allen verfügbaren WLANs suchen und müssen nicht auf gesendete Beacons warten. Dies ist insbesondere hilfreich im Roaming-Szenario: D. h. wenn ein unterbrechungsfreier Wechsel von einem BSS bzw. einer WLAN-Zelle in die nächste – unter Kontrolle des gleichen Anbieters – notwendig ist. Außerdem bietet der aktive Discovery-Mechanismus die einzige Möglichkeit, ein WLAN zu finden und sich damit zu verbinden, wenn es sich um einen AP mit einem versteckten WLAN-Namen (Hidden SSID, siehe hierzu Abschnitt 5.1.2) handelt.

Alle SSIDs, die dem Nutzerendgerät durch das passive oder aktive Verfahren mitgeteilt werden, werden schließlich den WLAN-Nutzenden angezeigt. Diese können nun das gewünschte WLAN auswählen. Falls das gewählte WLAN nicht offen betrieben wird, werden die Nutzenden zum Zweck der Authentifizierung nach einem Passwort gefragt.

Dafür müssen sie eine Einstiegsseite im Web-Browser öffnen. Auf dieser sind in vielen Fällen neben der Passwort-Anfrage auch die Allgemeinen Geschäftsbedingungen (AGBs) sowie die Datenschutzerklärung des WLAN-Betreibers zugänglich. Einstiegsseiten können ggf. auch als Registrierungsseite fungieren, über die neue WLAN-Nutzende ihr Benutzerkonto anlegen können. Der Anmeldeprozess bzw. die einmalige Registrierung wird entweder durch den AP oder durch einen zusätzlichen Authentifizierungsserver (siehe Abb. 04) ausgeführt. Von WLAN-Betreibenden mit geringen finanziellen Mitteln (z. B. Cafés) wird nur selten eine WLAN-Infrastruktur mit zusätzlichem Authentifizierungsserver betrieben, da dies die Einrichtung und regelmäßige Wartung eines Servers erfordert. WLAN-Hotspot-Betreibende (also z. B. die Deutsche Telekom AG) setzen jedoch stets Einstiegsseiten ein. Dadurch soll sichergestellt werden, dass der Zugang zu der WLAN-Infrastruktur nur ausgewählten Kunden vorbehalten ist. Sobald die Authentifizierung erfolgreich durchgeführt ist, sind die Nutzenden mit dem AP verbunden und somit Teilnehmende des WLAN-Netzes.

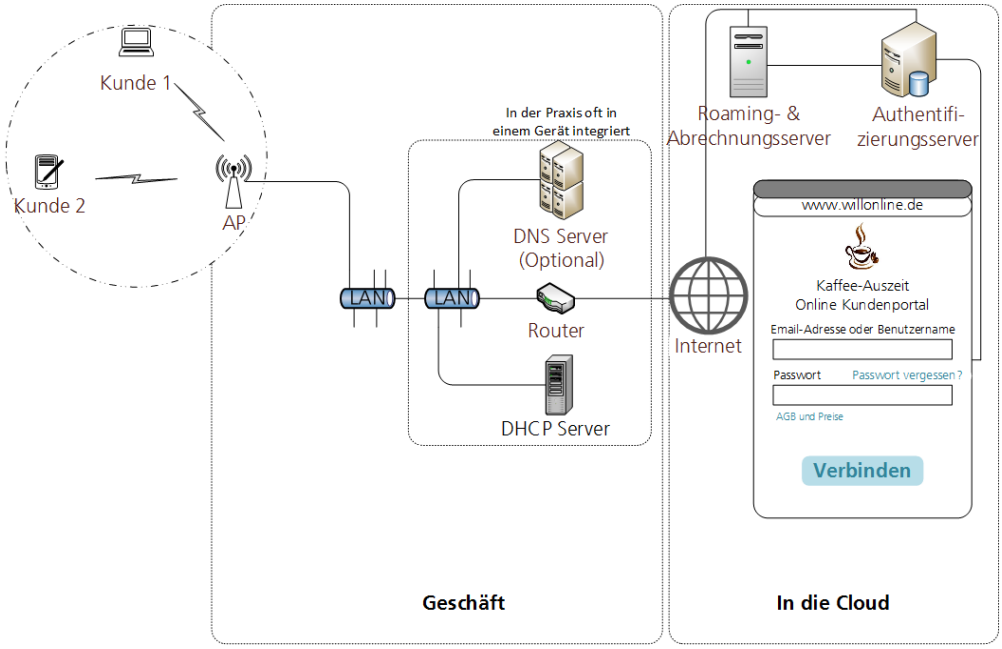

Abb. 04 Aufbau eines öffentlichen WLANs mit einem externen Authentifizierungsserver (auf dem u. a. die Benutzerkonten gespeichert sind) sowie einer Einstiegsseite

Netzwerkkonfiguration: Nachdem die WLAN-Nutzenden den AP gefunden haben und sich dort authentifiziert haben, wird ihnen eine IP-Adresse zugewiesen. Diese ist für die Kommunikation über das Internet unabdingbar. Die Zuweisung der IP-Adresse erfolgt in der Regel durch einen sog. Dynamic Host Configuration Server (DHCP-Server). Diese Netzwerkkonfiguration läuft vollständig automatisiert im Hintergrund ab. Dabei senden Nutzerendgeräte eine DHCP-Discover-Nachricht. Der DHCP-Server antwortet daraufhin mit einem DHCP-Offer. Damit teilt der DHCP-Server dem Nutzerendgerät die Netzwerkkonfigurationsdaten mit. Als nächstes gibt das Nutzerendgerät dem DHCP-Server bekannt, dass dieser nun die erhaltenen Konfigurationsdaten anwenden möchte. Dies geschieht mittels eines DHCP-Requests. Dieser wiederum wird im letzten Schritt seitens des DHCP-Servers bestätigt. Bei dieser Konfiguration durch den DHCP-Server wird dem Nutzerendgerät zudem die Adresse des Domain Name System-Servers (DNS-Servers) mitgeteilt. Der DNS-Server wird benötigt, um den Namen der Internetseite in die zugehörige IP-Adresse umzuwandeln. Zum Beispiel gibt der DNS-Server bei der Anfrage nach dem Namen *www.zdf.de* die IP-Adresse 91.197.29.78 zurück. Dieses System wurde eingeführt, da sich Menschen die Namen von Internetseiten besser merken können, während Router und Server numerische IP-Adressen benötigen, um entsprechende Internetseiten abrufen zu können. DHCP- und DNS-Server sind in der Regel im Router enthalten und befinden sich somit im selben Subnetz wie der WLAN-AP. Die Komponenten sind i. d. R. in einem Netzwerkgerät (WLAN-Router) verbaut und über eine LAN-Verbindung miteinander verbunden. Gewerbetreibende wie z. B. Hotel- oder Ca-

fébesitzer, die ihr WLAN ihrer Kundschaft oder Gästen zur Verfügung stellen oder mit einem kleinen Budget ausgestattete Unternehmen bzw. Institutionen betreiben daher zumeist lediglich einen WLAN-Router, der auf der einen Seite über eine Kabelverbindung an das Internet angeschlossen, und auf der anderen Seite über Funk mit den Nutzerendgeräten (WLAN-Clients) verbunden ist. Größeren Betreibenden (z. B. Kommunen, Einkaufzentren oder Flughäfen) reicht ein WLAN-AP allerdings nicht aus, um damit alle Stockwerke mit einem ausreichend starken und stabilen WLAN-Signal zu versorgen, oder flächendeckendes WLAN über größere Gebiete hinweg anzubieten. Zu diesem Zweck müssen mehrere APs und WLAN-Repeater eingesetzt werden. In solch einem Fall ist die Trennung der APs zum Router ersichtlicher, da die verschiedenen APs als eigenständige Geräte an verschiedenen Orten (z. B. Stockwerke im Einkaufszentrum) installiert werden. Die Verbindung der APs untereinander wiederum erfolgt entweder über eine LAN Verbindung (siehe Abb. 05) an die auch der Router angeschlossen ist oder über Funk (eine sog. *WDS-Verbindung*).

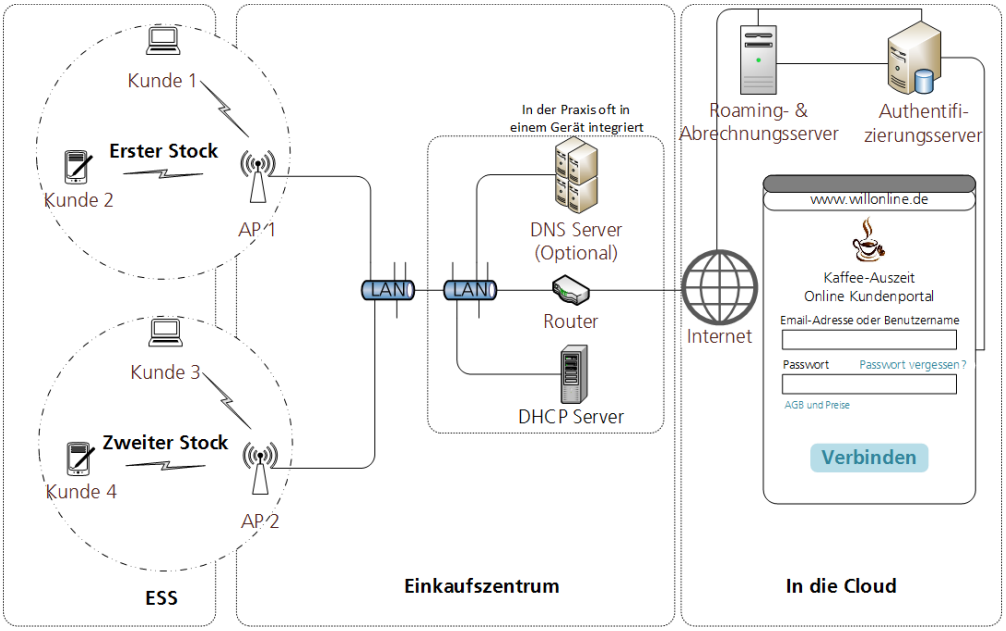

Abb. 05 Aufbau eines öffentlichen WLAN-Netzes, bestehend aus Authentifizierungsserver, Einstiegsseite und mehreren APs, um eine größere Fläche abdecken zu können. Die Abbildung zeigt die Verbindung der APs über LAN.

Nachdem nunmehr die technische Funktionsweise in Grundzügen erläutert ist, wird als nächstes die gesellschaftliche Rahmung öffentlicher WLANs kurz beschrieben.

2.3 Gesellschaftliche Rahmung

Die Bereitstellung von öffentlichem WLAN ist zumeist an die bestehende Infrastruktur des öffentlichen Raums gebunden. Wenn Stadtverwaltungen Internet-Nutzung an öffentlichen Plätzen ermöglichen oder Cafés WLAN anbieten, dann handelt es sich um Institutionen, deren Bauwerke den physischen, öffentlichen Raum konstituieren. Diese können öffentliche (hier im Sinne von staatlichen Einrichtungen, wie z. B. Behörden) wie auch private (im Sinne privatwirtschaftlicher Akteure, wie z. B. Café-Betreiber oder auch von Privatpersonen, die ihr WLAN für Außenstehende öffnen) Institutionen sein. *Öffentlicher Raum* bezieht sich also zunächst auf Räume, für die jedenfalls prinzipiell keine Zugangsbeschränkung für bestimmte Personen oder Personenkreise vorliegt: Sie sind im Prinzip für jede und jeden zugänglich.

Stellen die den öffentlichen Raum konstituierenden Akteure, Institutionen und Organisationen nun WLAN zum öffentlichen Gebrauch zur Verfügung, dann meint auch dies zunächst den unbeschränkten Zugang für Nutzende – keine Personengruppe o. ä. ist von der Nutzung prinzipiell ausgeschlossen. Insofern lässt sich hier also eine Parallele zum öffentlichen Raum ziehen, der zunächst einmal ebenfalls allen möglichen Klassen

von sozialen Akteuren zur Verfügung stehen soll (jedenfalls der normativen Idee nach): WLAN-Zugang zum Internet kann dann in gewissem Sinne als digitaler öffentlicher Raum gelten, worauf die Bezeichnung „öffentliches WLAN" ja auch hinweist.

Allerdings ist es sehr wahrscheinlich, dass WLAN-Nutzende, die sich im öffentlichen Stadtraum befinden, bspw. ein privates soziales Netzwerk-Profil aufrufen oder Online-Banking betreiben. In dem Fall würde die Kanalbildung zum Internet zwar über den öffentlichen Raum des öffentlichen WLANs erfolgen, der aufgesuchte *Ort* wäre indes eher von privatem Charakter.

In diesem Sinne wird hier deutlich, dass die Unterscheidung öffentlich/privat im vorliegenden Fall auf mehreren, sich überlagernden Ebenen Anwendung findet. Aus diesem Grund ist die Nutzung von öffentlichem WLAN im physischen öffentlichen Raum zu privaten Zwecken mit einigen Schwierigkeiten hinsichtlich der klaren Zuweisung von Verantwortlichkeiten für Datenschutz und Sicherheit behaftet (dies gilt zumindest in moralischer Hinsicht, und die gegenwärtig gewissermaßen erst „nachziehende" rechtliche Regulierung der Störerhaftung lässt sich als vielsagendes Symptom dafür verstehen):

- Sofern sich der Staat für die Sicherheit des physischen öffentlichen Raums verantwortlich zeichnet, könnte diesem auch die Verantwortung für die Sicherheit des per WLAN konstituierten virtuellen Raums zufallen.
- Oder sind es die jeweiligen Betreiber der Hotspots, die ja erst den WLAN-Raum konstituieren – immerhin sind ja auch z. B. Schwimmbad-Betreiber für die Einhaltung gewisser Sicherheitsstandards auf ihrem Gelände verantwortlich.
- Denkbar wäre auch die Zuweisung von Verantwortung an die Nutzenden selbst, so wie man sozialen Akteuren auch das Treffen gewisser Mindest-Vorkehrungen im physischen öffentlichen Raum zumutet (man kann den Staat kaum für mangelnde Sicherheitsvorkehrungen verantwortlich machen, wenn man bei roter Ampel vor ein Auto läuft, allerdings werden den am Straßenverkehr Teilnehmenden auch spätestens mit Eintritt in die Grundschule per Verkehrserziehung systematisch und flächendeckend Verhaltensregeln und Kompetenzen vermittelt).

Während die Listung der versch. Akteursgruppen hier eher exemplarisch als erschöpfend gedacht ist, kann die Frage, wie sich welche Verantwortlichkeiten auf welche der genannten Akteursgruppen verteilt, im Rahmen dieses White Papers nicht letztgültig beantwortet werden. Sie soll aber zumindest aufgeworfen werden, um die gesamtgesellschaftliche Verantwortung sichtbar zu machen, die hinsichtlich der fraglichen Infrastrukturen zu konstatieren ist. Denn es ist zum einen keinesfalls legitim, Daten, die im öffentlichen WLAN-Raum zirkulieren, einfach mit der Begründung abzugreifen, es handele sich hierbei ja um öffentlichen Raum: Erstens findet die Beschreibung „öffentlich" (wie oben ausgeführt) in diesem Falle ja in einem ganz spezifischen, mehrfach überlagerten Sinne Anwendung; und zweitens hegen Akteure im physischen öffentlichen Raum durchaus auch berechtige Privatheitserwartungen. Zum anderen kann dann aber auch die Verantwortlichkeit für Datenschutz und Sicherheit nicht jedem Einzelnen zugeschoben werden, sondern muss vermutlich auf verschiedene Schultern verteilt werden. Wie dies genau erfolgen könnte, bleibt zu diskutieren.

2.4 Akteursinteressen

In den Auseinandersetzungen um öffentliche WLANs treffen die Interessen sowohl öffentlicher als auch gewerblicher Akteure sowie privater Nutzerinnen und Nutzer aufeinander. Diese Perspektiven werden im Folgenden näher beleuchtet.

2.4.1 Vorteile aus Sicht kommunaler Akteure

Verschiedene Großstädte bieten derzeit bereits einzelne WLAN-Hotspots an öffentlichen Plätzen und in öffentlichen Gebäuden an. Darunter sind beispielsweise Städte wie München, Ulm, Karlsruhe, Freiburg, Berlin oder Augsburg. Die Finanzierung, Abdeckung, Nutzungsbeschränkungen sowie das Ausmaß des Zugriffs auf personenbezogene Daten variieren allerdings zum Teil erheblich von Stadt zu Stadt. In Berlin zum Beispiel können Nutzende zeitlich unbegrenzt und ohne Anmeldung an 650 WLAN-Zugangspunkten in und an öffentlichen Gebäuden auf das Internet zugreifen.[31] Die Stadt Ulm setzt dagegen vor der Nutzung eine Registrierung mit Namen und Mobilfunknummer bzw. E-Mail-Adresse voraus. Danach steht das WLAN für zwei Stunden mit unbegrenztem Datenvolumen zur Verfügung. Städtische Internetseiten sind jedoch häufig ohne Login verfügbar und können daher direkt von Einwohnern und Touristen genutzt werden, um schnell an relevante Informationen zu gelangen.[32]

Begründet wird die Bereitstellung des öffentlichen WLANs in Ulm etwa damit, dass WLAN „als Grundversorgung an wichtigen öffentlichen Plätzen“[33] betrachtet wird. Ein weiterer Ausbau sei außerdem „unabdingbare Voraussetzung einer modernen Stadtverwaltung“.[34] Während die Kosten hierbei von der Stadt Ulm selbst getragen werden, übernimmt die Finanzierung in Freiburg ein externer Anbieter. Dabei steht das WLAN in Ulm nur an öffentlichen Plätzen zur Verfügung, in Karlsruhe werden daneben noch zwei Stadtbahnen versorgt und in Freiburg besteht bereits ein flächendeckendes WLAN-Netz.[35]

Als weiteres, mit dem Grundversorgungsargument verwandtes, Argument für das Angebot von öffentlichem WLAN führen Städte und Kommunen an, die Unterschiede im Zugang zu und der Nutzung von Informations- und Kommunikationstechnologien (Stichwort: „Digital Divide“) überwinden zu wollen.[36] So soll mit dem Angebot von WLAN-Hotspots breiten Bevölkerungsgruppen der Zugang zum Internet ermöglicht werden. Neben den Einwohner/-innen der jeweiligen Kommune gehören dazu insbesondere sozial benachteiligte Randgruppen, die in der Regel nicht imstande sind, über einen eigenen Internetzugang zu verfügen, wie etwa Obdachlose, von Armut betroffene Menschen sowie Geflüchtete.[37]

Ein ganz anderes Argument für die Einrichtung von WLAN-Hotspots auf Kommunalebene stellt das Potenzial zur Effizienzsteigerung dar. Es wird beispielsweise damit argumentiert, dass Prozessabläufe durch das Angebot von öffentlichem WLAN verbessert werden könnten: So könnten sich Einwohnerinnen und Einwohner vor bzw. während Behördengängen über die jeweiligen Behördenabläufe informieren.[38] Ein Beispiel, wie Kommunen von öffentlichen WLAN-Angeboten profitieren können, stellt eine aktuelle App der Stadt Saarbrücken dar. Über diese können Einwohner/-innen der Stadt über das Kontakt- und Beschwerdemanagement mit der Kommune Kontakt aufnehmen, um etwa zuständige Behörden direkt über defekte Straßenlampen oder Schlaglöcher zu informieren.[39]

Als ein weiteres Argument für die Einrichtung von öffentlichen WLANs wird hervorgehoben, dass sich Städte und Kommunen durch dieses Angebot gegenüber anderen Gemeinden differenzieren können. So lasse sich mit dem Angebot von öffentlichen WLANs die Attraktivität der Kommune nicht nur für Einwohner/-innen, sondern insbesondere auch für Touristen steigern.[40] Städte und Kommunen versprechen sich von dem WLAN-Hotspot-Angebot, dass Bürger/-innen und Touristen die Stadt auf eine bessere Art und Weise erleben können. Die Bereitstellung von speziellen Webseiten und Apps soll zum Beispiel dazu dienen, dass sowohl Bewohner/-innen als auch Besucher/-innen schnell an relevante Informationen gelangen und dadurch die Infrastruktur und Angebote der Stadt intensiver nutzen können. Zum Beispiel können Städte das WLAN-Angebot nutzen, um spezielle Touristeninformationen bereitzustellen. Mit diesen Informationen können Städte die Besucher/-innen auf spezielle Attraktionen und Angebote aufmerksam machen, wie etwa nahegelegene Museen, Ausstellungen oder Restaurants.[41] So bietet beispielsweise die Stadt München mit der sogenannten „Mün-

chen App“ Inhalte, wie Sehenswürdigkeiten, Hotel- und Restaurantvorschläge mit Entfernungsangaben vom aktuellen Standort sowie einen integrierten Routenplaner.[42] Ein anderes aktuelles Beispiel liefert die Stadt Berlin. Sie stellt den Nutzerinnen und Nutzern städtischer WLAN-Hotspots die Interviewreihe „Typisch Berlin“ zur Verfügung. Zum Zwecke der Attraktivitätssteigerung der Stadt erläutern Berliner Persönlichkeiten darin, was die Hauptstadt für sie persönlich ausmacht.[43]

Es ist jedoch anzunehmen, dass derartige Differenzierungsversuche vor allem zu Beginn der Verbreitung von WLAN-Hotspots ein wesentliches Argument darstellen. Mit steigender Verbreitung öffentlicher WLAN-Angebote in Städten und Kommunen ist davon auszugehen, dass die Möglichkeit der Differenzierung wieder abnehmen wird.

2.4.2 Vorteile aus Sicht gewerblicher Anbieter

Neben Städten und Kommunen erhoffen sich auch gewerbliche Anbieter, wie Hotel-Restaurant- und Cafébetreiber sowie der Einzelhandel neue Vorteile vom WLAN-Angebot. Gewerbetreibende wollen zum Beispiel durch das Angebot eigener WLAN-Hotspots Umsatzsteigerungen erzielen. Sie rechnen damit, dass die Kundschaft durch die Möglichkeit der kostenlosen Internetnutzung länger vor Ort verweilt bzw. das Restaurant, Café oder die Einzelhandelsfiliale häufiger besucht.[44] Wenn Kundinnen und Kunden das Restaurant oder Café also nicht nur zum Essen und Trinken aufsuchen, sondern dabei die Möglichkeit zum Arbeiten oder Surfen im Internet nutzen, erhoffen sich die Betreiber, dass sie durch die längere Verweildauer auch mehr konsumieren.[45] Auch aus Sicht gewerblicher Anbieter stellt – gerade zu Beginn der Verbreitung von öffentlichen WLAN-Angeboten – das eigene Angebot eines WLAN-Hotspots eine Differenzierungsmöglichkeit gegenüber anderen Restaurant- oder Cafébetreibern dar. Entsprechend werden eigene WLAN-Hotspots bereits häufig als zusätzliches Leistungsangebot präsentiert und beworben.[46]

Speziell der Einzelhandel verspricht sich eine Reihe zusätzlicher Vorteile durch das eigene WLAN-Angebot. Anbieter können das öffentliche WLAN als Zusatzleistung erweitern, indem sie beispielsweise die Einstiegsseite so gestalten, dass die Nutzerinnen und Nutzer des WLANs direkt zu Produktinformationen oder Bewertungen geleitet werden. Dies ist attraktiv für Anbieter, da Produktrezensionen von anderen Kunden in der Regel einen positiven Einfluss auf die individuelle Kaufentscheidung haben.[47] So könnten sie etwa Anreize für Impulskäufe setzen, die durch die Nutzung des WLANs begünstigt werden.[48] Die Supermarktkette Tesco in Großbritannien bietet etwa die Möglichkeit über das eigene WLAN Gutscheine herunterzuladen, Produktinformationen einzusehen oder aktuelle Angebote des Supermarktes zu nutzen.[49] Auch Preisvergleiche könnten auf diese Weise integriert werden, um dem sogenannten Showrooming-Phänomen entgegenzuwirken. Dieses Phänomen beschreibt, dass ein Produkt zwar im Geschäft betrachtet und ggf. bereits die Kaufentscheidung getroffen wird, es jedoch dann häufig im Internet bei anderen Anbietern erworben wird, die das Produkt zu einem günstigeren Preis anbieten.[50]

Anbieter können sich zudem standortbezogene Dienste zu Nutze machen. Diese Dienste können der Kundschaft auf die aktuelle Aufenthaltsposition abgestimmte Informationen zur Verfügung stellen. Mithilfe des WLANs kann der Standort eines Kunden in innerhalb eines Supermarktes genau bestimmt und diesen in unmittelbarer Nähe befindliche Angebote angezeigt werden. Auch diese Angebote sollen dazu dienen, Impulskäufe anzuregen und sich somit umsatzsteigernd auswirken. Zudem können mit Hilfe des WLANs die Wege der Kundschaft innerhalb des Geschäfts aufgezeichnet und so das Einkaufsverhalten analysiert werden – zumindest sofern der WLAN-Adapter am Smartphone eingeschaltet bleibt.[51] Die Supermarktkette Tesco hat das Verfahren noch weiter optimiert und zieht bereits getätigte Käufe ihrer Kunden ebenfalls in die Angebotsempfehlungen mit ein. Wurde beispielsweise beim letzten Einkauf eine bestimmte Marke Butter gekauft, die zurzeit reduziert angeboten wird, macht Tesco über das

eigene WLAN auf dieses Angebot aufmerksam und navigiert die betreffende Person zu dem Produkt.[52]

Derartiges Profiling ist zugleich ein Beispiel dafür, wie ein Unternehmen die Daten der Kundschaft nutzen kann, um spezielle Angebote zu versenden. Je nach Authentifizierungsart erfasst das Unternehmen auch E-Mail-Adressen, die zu Werbezwecken (z. B. Newsletter) genutzt werden können.[53] Außerdem besteht grundsätzlich die Möglichkeit, den Browserverlauf der Nutzenden auszuwerten. Auf Basis dieser Auswertungen könnten Anbieter das eigene Angebot entsprechend anpassen. Besucht eine Kundin oder ein Kunde während des Einkaufs in der Filiale über das angebotene WLAN die Webseite der Konkurrenz und bestellt dort Produkte, die nicht im eigenen Sortiment enthalten sind, kann das Wissen darüber zur Erweiterung des eigenen Sortiments um die entsprechenden Produkte genutzt werden.[54]

2.4.3 Mögliche Vorteile für Nutzerinnen und Nutzer

Neben Vorteilen für Anbieter kann das Angebot von öffentlichem WLAN auch aus Sicht der Nutzerinnen und Nutzer verschiedene Vorteile bieten. Der zentrale Vorteil besteht natürlich darin, dass bei der Internetnutzung nicht mehr auf das – häufig begrenzte und vergleichsweise langsame – mobile Datenvolumen des eigenen Mobilfunkanbieters zurückgegriffen werden muss. Außerdem ist die mobile Datenverbindung in Gebäuden oftmals instabil, wohingegen der Zugang über das angebotene WLAN eine zuverlässigere und schnellere Internetverbindung ermöglicht.[55]. Dieses Angebot kann den Alltag von Kundschaft und Besucher(inne)n erleichtern, da sie über das WLAN Informationen und datenintensive Medienangebote aus dem Internet abrufen können. Insbesondere die Interaktion mit anderen Personen über soziale Netzwerke (z. B. Facebook, Snapchat oder Instagram) oder internetbasierte Sofortnachrichtendienste, wie Threema, WhatsApp oder Telegram, kann dadurch komfortabler werden.[56]

WLAN-Angebote im Einzelhandel zielen darauf ab, ein verbessertes Einkaufs-Erlebnis für die Kundschaft zu schaffen, das diese als Vorteil gegenüber dem Angebot in anderen Geschäften wahrnehmen können. Durch den Zugang zu Informationen im Internet kann zum Beispiel auf spezielle Angebote, Preisvergleiche, Produktinformationen, Bewertungen oder Loyalitätsprogramme des jeweiligen Einzelhandelsgeschäfts zugegriffen werden. DM-Drogeriemarkt-Filialen bieten ihrer Kundschaft etwa die Möglichkeit, Coupons für das angebotene Loyalitätsprogramm (Payback) über das in der Filiale frei verfügbare WLAN herunterzuladen.[57] Zudem können von DM angebotene Apps heruntergeladen werden, die den Einkauf unterstützen sollen.[58] Über eine eigene App („Foto2Go-App“) können Fotos kabellos vom Smartphone auf die Geräte vor Ort übertragen, Fotobücher gestaltet und das Drucken von Abzügen vorbereitet werden.

Für Angestellte und Geschäftspersonen kann die Verfügbarkeit eines freien WLANs eine Alternative zum Büro oder dem Home-Office darstellen. So können Wartezeiten vor Terminen oder während Geschäftsreisen durch öffentliches WLAN an Flughäfen, in öffentlichen Verkehrsmitteln oder Cafés dazu genutzt werden, um der Arbeit nachzugehen, E-Mails abzuarbeiten, Informationen aus dem Internet abzurufen oder Videotelefonate zu führen.[59]

Touristen stellen eine weitere Personengruppe dar, die vom Angebot öffentlicher WLANs profitieren kann. Da Touristen aus dem Ausland zumeist ausschließlich ausländische Mobilfunkverträge haben, würden durch die Nutzung des eigenen Datenvolumens Roaming-Gebühren anfallen. Durch öffentliches WLAN kann dieser Personenkreis von Kosteneinsparungen profitieren indem etwa Angehörige und Freunde über Sofortnachrichtendienste kostenfrei kontaktiert oder soziale Netzwerke genutzt werden können. Zudem können Touristen auf abgestimmte Informationen vor Ort, wie etwa Kartenmaterial, Routenempfehlungen oder Empfehlungen für Aktivitäten oder Restaurants zugreifen.[60]

Der für Nutzerinnen und Nutzer bequemste Zugang zum öffentlichen WLAN ist über offene und über freie WLANs möglich, bei denen weder Passwörter benötigt werden noch Gebühren anfallen. Freifunk ist ein Verein, der solches freies WLAN für die Öffentlichkeit anbietet. Somit können alle, die sich in der Nähe eines Freifunknetzes befinden, über dieses Netz ins Internet gelangen. Für die Bereitstellung des Freifunknetzes wird auch auf die Öffentlichkeit gesetzt. Hierfür könne alle, die ein Freifunknetz anbieten wollen, eine kostenfreie Software von Freifunk beziehen. Diese Software muss dann auf den eigenen oder einen zusätzlichen Router installiert werden, wodurch ein freies WLAN über den eigenen Internetanschluss angeboten wird. Dieser Internetzugang ist fortan Teil des Freifunknetzes und kann von jeder Person kostenfrei genutzt werden, die sich in der Nähe eines Freifunk-APs befindet.

2.4.4 Zwischenfazit

Immer mehr Städte und Kommunen als auch gewerbliche Anbieter stellen ihren Einwohner/-innen und Besucher/-innen bzw. ihrer Kundschaft kostenfreies öffentliches WLAN zur Verfügung.

Öffentliche Akteure wollen damit sowohl eine Grundversorgung der Bevölkerung mit einem Internetanschluss gewährleisten als auch die Stadt oder Kommune mit diesem Angebot gegenüber anderen Regionen positiv abheben und damit Touristen anlocken. Gewerbliche Akteure wiederum versprechen sich durch die Zurverfügungstellung kostenfreier öffentlicher WLANs Umsatzsteigerungen, indem die Kundschaft vor allem effektiver zum Kauf oder einer längeren Verweildauer und damit erhöhtem Konsum angeregt wird. Sowohl bei öffentlichen als auch gewerblichen Akteuren variiert die Qualität, Geschwindigkeit usw. des angebotenen kostenfreien WLANs mitunter enorm. Für die Nutzenden ist zumindest die Möglichkeit eines kostenlosen Internetzugangs – aufgrund des damit verbundenen Komfortgewinns – attraktiv.

Der behauptete Kundennutzen durch die Anbieter ist allerdings kritisch zu sehen. Deshalb ist zu fragen, aus welchen anderen Motiven WLANs angeboten werden und was diese Motive und davon ausgehenden Praktiken vor allem für Sicherheit und Datenschutz bedeuten. Denn neben der eingangs erwähnten Problematik der Störerhaftung, aufgrund derer in Deutschland nur wenige öffentliche und noch weniger offene und/oder freie WLANs zur Verfügung stehen, besteht eine weitere große Problematik in Bezug auf die Gewährleistung von Datenschutz und Privatheit in öffentlichen WLANs. Derlei Privatheitsbedenken existieren nicht nur in Bezug auf technische Ausspähmöglichkeiten, die von beliebigen Tätern ausgenutzt werden können sondern insbesondere aufgrund der Praktiken von WLAN-Betreibenden, die tiefgehende Einblicke in das Privatleben sowohl von WLAN-Nutzenden als auch jenen, die diese Netzwerke nicht verwenden, jedoch ihren WLAN-Adapter am Smartphone außerhalb der eigenen vier Wände nicht abschalten, erlauben. Derartige Praktiken werden im folgenden Abschnitt beschrieben und diskutiert.

3 Bedrohungs- und Überwachungspotenziale in öffentlichen WLANs

Nachdem in Abschnitt 2.2 der Aufbau und die Funktionsweise von WLANs überblicksartig beschrieben wurden, widmet sich dieser Abschnitt den technischen Bedrohungen. Dabei wird eine Differenzierung möglicher Angreifer (Angriffsmodelle) erarbeitet sowie erläutert, über welche Motivation, Fähigkeiten und Zugriffsmöglichkeiten Angreifer verfügen (Abschnitt 3.1). Im Anschluss werden (Überwachungs-)Praktiken der Betreiber öffentlicher WLANs beschrieben und welche Auswirkungen daraus für die Privatheit der WLAN-Nutzenden erwachsen können. (Abschnitt 3.2).

3.1 Angriffsmodelle – Angriffstypen und Bedrohungsursachen

Eine hilfreiche Methode für die Analyse von Bedrohungen für IT-Sicherheit (Daten- und Systemsicherheit) und Privatheit stellt die Modellierung verschiedener Angreifer dar. Dabei werden unterschiedliche Angriffstypen, gegen die sich WLAN-Nutzende und Infrastrukturbetreibende schützen müssen, identifiziert. Unter dem Begriff Bedrohung wird dabei i. d. R. ein Umstand bzw. ein Ereignis bezeichnet, durch das Schaden für Betreiber und/oder Nutzende eines IT-Systems entstehen kann.[61] Derartige Bedrohungen sind zumeist entweder auf Schwachstellen (wie fehlerhafte Design-Entscheidungen und Implementierungs- bzw. Konfigurationsfehler) in der WLAN-Infrastruktur oder auf obskure Geschäftspraktiken der WLAN-Anbieter zurückzuführen.

Grundsätzlich kann von zwei Angriffsmodellen ausgegangen werden. Diese unterscheiden sich hinsichtlich der Fähigkeiten der Angreifer:

- Angriffsmodell, das von aktiven Angreifern ausgeht (siehe 3.1.1) und,
- Angriffsmodell, das von passiven Angreifern (siehe 3.1.2) ausgeht.

Angreifer können allerdings auch abhängig von ihrer Stellung im WLAN kategorisiert werden. So können Entitäten, die sich auf dem Kommunikationspfad zwischen WLAN-Client und Onlinediensten befinden, als passive Angreifer bzw. aktive Angreifer fungieren. Derartige Angreifer, auch On-Path-Angreifer genannt, können diese Rolle wahrnehmen, weil sie beispielweise für die Vermittlung von Datenpaketen zuständig sind oder die ausgetauschten Nachrichten abfangen können. Auch WLAN-Betreibende und Internet Service Provider (ISPs) können aufgrund ihrer Stellung in WLANs als potentielle On-Path-Angreifer betrachtet werden. Off-Path-Angreifer, d. h. Angreifer die keinen direkten Zugriff auf die ausgetauschten Nachrichten haben, treten als Pendant zu On-Path-Angreifern auf. Durch Einsatz geeigneter Techniken (z. B. HTTP-Session-Hijacking durch Angreifer aus demselben Netzsegment; Hintertüren in Routern[62]) oder zusätzlicher Hardware (z. B. Evil Twins – s. u.) können sich Off-Path-Angreifer in einen Kommunikationspfad einklinken und so de facto zu einem On-Path-Angreifer werden.

3.1.1 Passive Angriffsmöglichkeiten

Als On-Path-Angreifer können passive Angreifer die Kommunikation im WLAN bzw. den Datenaustauch mit Online-Diensten mithören und für spätere Zwecke aufzeichnen. Allerdings kann der beobachtete Datenstrom nicht verändert, umgeleitet oder deren Zustellung verhindert werden. Demnach können ISPs, Hard- bzw. Software-Hersteller, WLAN-Betreibende, Wartungstechniker, andere WLAN-Nutzende, aber auch sonstige Außenstehende (z. B. unautorisierte (nicht-)staatliche Akteure) als potentielle passive Angreifer betrachtet werden. Diese können sowohl unabhängig als auch abhängig

voneinander agieren bzw. auftreten. Passive Angriffe entstehen i. d. R. durch die Ausnutzung fehlerhafter Design-Entscheidungen in IEEE 802.11 (z. B. fehlende Verschlüsselung der Probe Requests) oder Implementierungs- bzw. Konfigurationsfehler im WLAN-Router (Schwachstellen bzw. Hintertüren oder eine unverschlüsselte Datenübertragung zwischen WLAN-Client und Router). Dadurch wird ausschließlich die Vertraulichkeit der Kommunikation im WLAN beeinträchtigt.

Abhören der Luftschnittstelle (vor dem Aufbau der Verbindung mit AP)

Nach der IEEE 802.11-Norm muss jede Probe Request-Nachricht an den AP im Klartext gesendet werden. Demnach kann jede Entität in Funkreichweite bzw. im lokalen Netz mit wenig Aufwand alle ausgesendeten Probe Requests empfangen und sammeln. Dafür muss das Gerät der passiven Angreifer mit entsprechend leicht zugänglicher Software ausgerüstet sein und der WLAN-Adapter sich im sog. *Monitor-Modus* befinden. Durch das Abfangen des Probe Requests können passive Angreifer Informationen über alle WLAN-Clients in der Funkzelle einsehen. Hierzu zählen etwa MAC- und IP-Adressen, die SSIDs mit denen ein Gerät in der Vergangenheit verbunden war, sowie die Signalstärke der aktuellen Verbindung. Aus den hierdurch gewonnenen Daten lassen sich weitere sensible Informationen der jeweiligen Nutzenden (oder Besitzer/-innen der WLAN-Clients) ableiten. So kann beispielweise eine Verknüpfung der MAC-Adresse und Signalstärke dazu verwendet werden, die Geräteposition zu bestimmen. Die Lokalisierung von mobilen Endgeräten in Gebäuden (Kaufhäuser, Messehallen, usw.) mittels MAC-Adressen und WLAN-Signalen stellt sogar die Grundlage neuartiger standortbasierter Dienste (englisch *location-based services*) wie Indoor-Navigation bzw. -Tracking und Indoor Analytics dar.[63] Mittels MAC-Adresse und Signalstärke aus den Probe Request-Nachrichten lässt sich die genaue Position eines Gerätes sowie das Verhalten der Nutzenden ermitteln.[64] Des Weiteren lassen sich aus der Verknüpfung der Liste aller SSIDs, mit denen ein Gerät in der Vergangenheit verbunden war (vgl. Abb. 06), mit Zusatzwissen aus anderen Datenbanken oftmals weitere Informationen beziehen, wie z. B. welches Transportmittel genutzt wurde (z. B. die SSID „WIFIonICE“ für WLANs in Zügen der Deutschen Bahn), in welchen Hotels das Opfer war („Pentahotel Brussels City Center“) oder welche Veranstaltungen besucht wurden („ForumPrivatheit_WLAN“).[65]

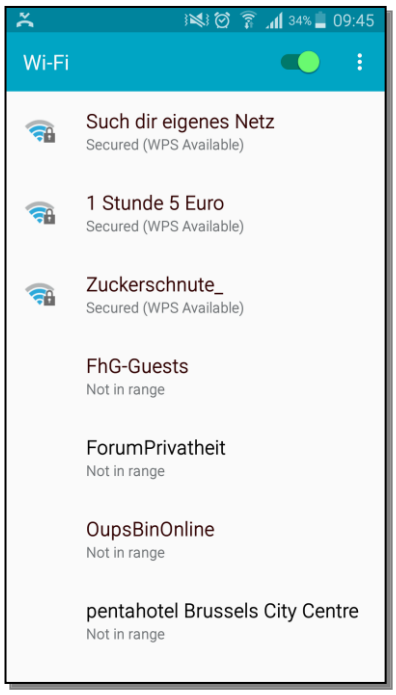

Abb. 06 Beispiel einer SSID-History

Angreifer, die Abhörgeräte in der Nähe unterschiedlicher öffentlicher Hotspots installieren oder auf mehrere APs oder Router zugreifen können (wie z. B. die Betreiber landes- bzw. bundesweiter öffentlicher Hot-Spots), sind in der Lage, die gesammelten SSIDs und MAC-Adressen zu nutzen, um Bewegungsprofile der Opfer über geografische Grenzen hinweg zu erstellen. Aus derartigen Datenverknüpfungen lassen sich auch Hinweise über Begegnungen und soziale Beziehungen zwischen Individuen ableiten.[66]

Abhören der Luftschnittstelle (nach dem Aufbau der Verbindung mit dem AP)

Ist die Verbindung mit dem WLAN-AP aufgebaut und die Nutzerin bzw. der Nutzer authentifiziert, können passive Angreifer fehlerhafte Sicherheitskonfigurationen des APs ausnutzen, um den Datenaustauch zwischen WLAN-Clients und dem AP bzw. zwischen WLAN-Clients und Online-Diensten mitzuhören und aufzuzeichnen. Konkret können hier Entitäten/Nutzende im gleichen Funknetz mögliche Sicherheitslücken und Fehlkonfigurationen im AP (z. B. unverschlüsselte bzw. lediglich WEP-verschlüsselte

Datenübertragung oder Nutzung des werkseitig voreingestellten Passworts) ausnutzen, um übertragene Datenpakete, d. h. jegliche Kommunikation, die über den WLAN-AP läuft, aufzuzeichnen. In öffentlichen WLANs werden häufig kaum oder nur schwache Sicherheitsmechanismen wie z. B. WEP oder WPA eingesetzt. Dahinter steckt die Motivation, WLAN-Nutzenden einen möglichst schnellen und reibungslosen Internetzugang zu ermöglichen. Aus der Analyse der abgefangenen Datenströme lassen sich allerdings Informationen, wie etwa Identifier bzw. IP-Adresse des Nutzerendgerätes und Zieladressen (IP-Adresse des Servers, also z. B. der Webseite, die besucht werden soll bzw. besucht wurde), Zeitpunkte und Länge der Interaktion mit den jeweiligen Online-Diensten ableiten. Eine Analyse dieser Verkehrsdaten ermöglicht Rückschlüsse über das Kommunikationsverhalten und Standorte sowie mit Hilfe einfacher Analysemethoden auch Rückschlüsse über soziale Beziehungen oder die Gesundheit der Nutzenden.[67] Zudem können passive Angreifer eine schwache Verschlüsselung der Datenübertragung zum WLAN-AP brechen.[68] Dadurch können sie die Inhaltsdaten extrahieren, also jene bei einer Kommunikation transportierten Daten abgreifen, die den konkreten und möglicherweise auch sensiblen Inhalt der Kommunikation bilden, wie z. B. Passwörter, Kreditkartennummern, E-Mail-Nachrichten oder interne Informationen von Unternehmen oder Behörden. Neben dem Abhören der Luftschnittstelle gibt es weitere Möglichkeiten für passive Angriffe, die entweder auf der Ausnutzung von Zugriffsrechten auf das System oder auf Hintertüren bzw. Schwachstellen im Router basieren[69] und die Abhörung des gesamten Datenverkehrs zwischen WLAN-Client und Online-Diensten erlauben. Beispiele hierfür sind u. a. die WLAN-Betreibenden selbst, Wartungstechniker, ISPs, Hard- bzw. Software-Hersteller aber auch sonstige Außenstehende (z. B. unautorisierte (nicht-)staatliche Akteure).[70] Sofern kompromittierte Zugangspunkte bzw. APs (malicious APs) nicht zum Zwecke von Denial of Service-Angriffen (DoS-Angriffen) eingesetzt werden, die eine Beeinträchtigung des Router-Dienstbetriebs zur Folge haben, können sie i. d. R. von den WLAN-Nutzenden nicht als solche wahrgenommen werden. Dies kann schwerwiegende Konsequenzen für die Privatheit haben.

Bei unverschlüsselter bzw. schwach verschlüsselter Datenübertragung können passive Angreifer darüber hinaus auch einen sog. *Session Hijacking-Angriff* (genauer, einen *HTTP Cookie Hijacking-Angriff*) durchführen.[71] Dabei wird die ungeschützt übertragene Session-ID (in Form eines HTTP-Cookies) abgefangen. Die Session-ID wird bei jeder Anfrage und Antwort zwischen WLAN-Client und Online-Dienst übertragen. Sie dient i. d. R. als Authentifizierungsmerkmal für die Dauer einer Sitzung. Angreifer können die gestohlene Session-ID dazu nutzen, um sich bei dem entsprechenden Online-Dienst z. B. Facebook als das Opfer auszugeben. HTTP Cookie Hijacking-Angriffe können zwar durch die Verschlüsselung des Kommunikationskanals (mittels HTTPS) unterbunden werden, fehlerhafte Umsetzungen in der Praxis ermöglichen es Angreifern jedoch auch weiterhin, auf die in der jeweiligen HTTP-Session erzeugten Cookies zuzugreifen.[72] Konkret wird bei HTTPS-Verbindungen meist zunächst eine unverschlüsselte HTTP-Sitzung erzeugt und darauf dann eine HTTPS-Sitzung aufgesetzt. Beim Übergang von HTTP zu HTTPS wird dann häufig dieselbe anfällige HTTP-Session weiterverwendet, weshalb selbst die Verwendung von HTTPS nicht in jedem Fall eine verlässliche Sicherheit bietet.

3.1.2 Aktive Angriffsmöglichkeiten

Grundsätzlich können aktive Angreifer größeren Schaden verursachen als passive Angreifer. Während sich passive Angreifer auf das Abhören und Abspeichern des Datenverkehrs im WLAN beschränken, können aktive Angreifer explizit in die Kommunikation eingreifen und die Integrität des Datenverkehrs kompromittieren. Das heißt, dass bei einem aktiven Angriff die gesendeten Nachrichten geändert, erweitert, umgeleitet, gelöscht, die Funk- bzw. Internetverbindung beendet oder gar fremde Inhalte auf dem Gerät des Opfers ausgeführt werden können.[73]

Zur Durchführung solcher Angriffe können beispielsweise Sicherheitslücken in der WLAN-Einstiegsseite,[74] in der eingesetzten Verschlüsselungsmethode für die Funküber-

tragung[75] oder in Routern[76] dazu ausgenutzt werden, um Skripte, aktive Inhalte und andere sog. Perma-Cookies (permanente Cookies)[77] in das WLAN einzuschleusen. Aktive Inhalte, Perma-Cookies und fremder, bösartiger Code dienen dazu, die Internetaktivitäten eines Opfers nachzuverfolgen und zu verketten, unerwünschte Werbung im Browser einzublenden und Angriffe auf das Nutzerendgerät zu starten (z. B. durch Einschleusen eines Trojaners). Als potentielle aktive Angreifer können sowohl Akteure auf dem Kommunikationspfad (z. B. WLAN-Betreibende, Wartungstechniker, ISP, Hard- bzw. Software-Hersteller) als auch Außenstehende (z. B. unautorisierte (nicht-)staatliche Akteure) agieren. Neben dem Zugriff auf den normalen Kommunikationspfad können aktive Angreifer aber auch zusätzliche WLAN-APs bereitstellen. Dadurch sind sie in der Lage, sich als Teil der legitimen WLAN-Infrastruktur auszugeben und so die Vertraulichkeit und Integrität des gesamten Netzverkehrs zu beeinträchtigen. Hierbei spricht man von sog. *Evil Twins* (böse Zwillinge), die als *Man-in-the-Middle* (MITM bzw. Mittelsmann) zwischen WLAN-Clients und Online-Diensten operieren.

3.1.3 Evil Twin-Zugangspunkte

Evil Twins sind gefälschte WLAN-Zugangspunkte (bzw. gefälschte APs), die seitens der Angreifer entweder im Funkbereich eines legitimen APs platziert oder ad-hoc an beliebigen Orten betrieben werden können. Als gefälschter AP wird ein Evil Twin typischerweise mit demselben Netzwerknamen (SSID) wie der legitime AP sowie mit gefälschten Sicherheitseigenschaften (z. B. gefälschte Zertifikate für die Einstiegsseite) und oft ohne Verschlüsselung betrieben. Um WLAN-Clients dazu zu bringen, sich mit einem solchen Evil Twin zu verbinden, senden diese ihre Beacons mit einem stärkeren Signal und/oder in kürzeren Abständen aus. Begünstigt wird diese Form der Attacke dadurch, dass sich ein WLAN-Client bei mehreren APs, die den gleichen Netzwerknamen haben, immer mit dem Zugangspunkt mit dem stärksten Signal verbindet. Verwenden Angreifer nun ein Tool, wie zum Beispiel aircrack-ng[78], ist es ihnen möglich, sogenannte „deauth" Datenpakete zu versenden. Diese speziellen Datenpakete werden normalerweise vom legitimen AP selbst versenden, um den WLAN-Clients mitzuteilen, dass die Funkverbindung getrennt wurde. Da die MAC-Adresse sowohl des APs als auch die des Clients bekannt ist bzw. sich leicht aus Probe Requests extrahieren lässt, können Angreifer „deauth" Pakete selbst erzeugen und aussenden. Nach dem Erhalt eines solchen Pakets baut der WLAN-Client eine neue Funkverbindung mit dem Evil Twin statt mit dem legitimen AP auf, falls dieser eine höhere Signalstärke hat.

Zudem können Evil Twin-Angreifer die Tatsache ausnutzen, dass WLAN-Clients regelmäßig Probe Requests mit allen ihnen bekannten Netzwerknamen (SSIDs) aussenden, solange der WLAN-Adapter am Gerät aktiviert ist. Diese können vom Angreifer mitgelesen werden, um anschließend einen Evil Twin-AP mit einer dem Client bekannten SSID ad-hoc zu betreiben. Dieses Vorgehen lässt sich mit entsprechender Software (z. B. hostapd[79]) sogar automatisieren. Hierbei wird dem Opfer ggf. eine Fälschung der Einstiegsseite angezeigt. Derartige Angriffe werden zudem dadurch begünstigt, dass die in dem Zusammenhang erzeugten Sicherheitswarnungen (z. B. Warnungen bei selbstsignierten SSL-Zertifikaten) von Nutzenden nicht immer korrekt eingeordnet und befolgt werden.[80]

Daneben wirkt auch die Notwendigkeit des Roaming-Verfahrens begünstigend für Evil Twin-Angriffe. Im 802.11-Standard bezeichnet Roaming ein Verfahren, das es WLAN-Clients ermöglicht, ohne aufwändige Neuanmeldung von einem AP zum nächsten im gleichen WLAN-Netzwerk umzuschalten, Dies ist immer dann hilfreich, wenn sich WLAN-Nutzende etwa in größeren Gebäuden frei bewegen und zugleich das WLAN ohne Unterbrechung nutzen wollen. Je nach Größe des Gebäudes müssen dazu unterschiedlich viele Zugangspunkte in regelmäßigem Abstand zueinander sowie mit identischer SSID und Einstellungen installiert werden, Verlässt ein WLAN-Client nun den Funkbereich eines Zugangspunktes, verbindet er sich automatisch mit dem nächsten verfügbaren Access Point mit der gleichen SSID. Da alle Access Points jeweils eine andere MAC-Adresse haben, basiert die Entscheidung für einen Verbindungsaufbau in aller

Regel auf der Erkennung der SSID. Angreifer können dies ausnutzen, um die SSID der legitimen APs zu kopieren und somit einen Evil Twin-Zugangspunkt aufzusetzen, mit dem sich ein Client automatisch verbindet.

Neben der Möglichkeit, den Evil Twin-AP in der Näher des legitimen APs zu platzieren, um den Funkverkehr von diesem umzuleiten, können Angreifer somit auch einen Verbindungszusammenbruch mit dem legitimen AP selbst in die Wege leiten, um im Anschluss den legitimen AP zu ersetzen.

Evil Twin-APs als Software- bzw. Hardware-Komponente

Für den Evil Twin-Angriff kann der gefälschte Zugangspunkt entweder als Software-Komponente oder in Form von Hardware realisiert werden.

Ein hardwarebasierter Angriff kann etwa bereits mit einem handelsüblichen WLAN-Router und einer modifizierten Firmware[81] erfolgen. Die Vorteile für die Angreifer sind dabei eine vergleichsweise starke Sendeleistung und hohe Bandbreite. Allerdings benötigen solche Geräte meist relativ viel Strom sowie eine Stromversorgung mit 12V. Dies und die Größe des Geräts schränken die Mobilität der Angreifer stark ein.

Im Unterschied zu den 802.11-Hardware-Lösungen bieten softwarebasierte Evil Twin-Zugangspunkte eine höhere Mobilität sowie die Möglichkeit den Angriff unauffällig mit einem Laptop oder, je nach verwendeter Software, sogar mit einem Smartphone zu starten. Softwarebasierte Evil Twin-APs können mit einer Vielzahl frei zugänglicher Software realisiert werden.[82]

3.2 Bedrohungspotenzial von Seiten gewerblicher und öffentlicher Akteure

Wie in Abschnitt 2.4 ausgeführt, besteht insbesondere auf Seiten privatwirtschaftlicher Anbieter ein großes Interesse an der Bereitstellung öffentlicher WLANs. Neben Vorteilen, wie der erhofften Verbesserung der Kundenbindung oder der Möglichkeit der Beeinflussung der Kaufentscheidung durch spezielle Einstiegsseiten, versprechen sich privatwirtschaftliche Anbieter eine Reihe von weiteren profitmaximierenden Vorteilen. Fortschrittliche Big Data-Analysetools sollen dabei helfen herauszufinden, wie viele und welche Art von Kunden welche Geschäfte betreten, was sie dort kaufen oder tun und wie sie dazu gebracht werden können, mehr Geld auszugeben ohne z. B. auf Online-Händler oder die Konkurrenz auszuweichen.[83]

Diese Art der Datenanalyse muss allerdings stets im Kontext umfassend und zunehmend digitalisierter Umgebungen verstanden werden. Schließlich werden in den seltensten Fällen Daten an ein und demselben Ort erhoben und analysiert. Stattdessen finden Datenerhebungen an unterschiedlichen Orten und zu unterschiedlichen Zeiten statt. Die Datenanalyse erfolgt nicht lokal, sondern in dafür vorgesehen Hochleistungsdatenzentren der jeweiligen Anbieter, die über den Globus verteilt sein können. Der unmittelbare Zusammenhang zwischen Erhebung und Verwendung von Daten rückt schließlich in Zeiten von Big Data-Analysen, in denen das Ziel gerade darin besteht, aus einer Vielzahl von unterschiedlichen Daten immer wieder neues, unerwartetes Wissen abzuleiten, zunehmend in den Hintergrund. Damit dieses Wissen wiederum möglichst schnell angezeigt werden und zu unmittelbaren Ergebnissen in der Geschäftspraxis führen kann, wird zugleich die Möglichkeit geschaffen, auf Cloud-Infrastrukturen zurückzugreifen. Da allerdings die wenigsten Geschäftsinhaber selbst über derlei Möglichkeiten verfügen, bieten inzwischen eine Reihe von Unternehmen ihre Dienste zum Zwecke der Kundenanalyse an. Diese Unternehmen, z. B. ShopperTrak, RetailNext, Nomi, Prism Skylabs oder Euclid Analytics schalten sich als Intermediäre zwischen die Nutzenden sowie die Geschäfte, in deren Auftrag sie die Kundendaten analysieren. Wurden Kundeninteressen bislang noch mithilfe von Bonusprogrammen wie Payback

und Kundenströme mithilfe von Wärmesensoren gemessen, bieten sich in Folge der Zunahme von Smartphones mit WLAN- und Bluetooth-Kapazität sowie der zunehmenden Verbreitung von Miniatursensoren (z. B. Bewegungs- bzw. Annäherungssensoren), die sowohl als eigenes Produkt vertrieben werden können als auch in bereits bestehende Produkte als Zusatzfeature integriert werden können, zahlreiche neue Möglichkeiten der Kundenanalyse an.[84] Die Vertreiber solcher Technologien und Geschäftsleute, die sie einsetzen argumentieren, dass damit ein Ausgleich im Machtgefälle zwischen physischem Einzelhandel und Online-Händlern möglich sei, das sich in den vergangenen Jahrzehnten zunächst einseitig zugunsten der Online-Händler entwickelt habe. Letztere hätten mithilfe von Kundentracking sowohl im virtuellen Shop (z. B. auf Basis von Perma-Cookies) als auch über Shop-Grenzen hinweg (auf Basis von MAC-Adressen) und der daraus resultierenden enormen Datenbasis einen gewaltigen Wissensvorsprung darüber erzielen können, welche Produkte bei ihrer Kundschaft besonders beliebt sind, welche auf der eigenen Plattform eingekauft werden und in welchen Fällen und warum ein Kauf scheitert bzw. bei der Konkurrenz erfolgt.[85]

Kundentracking auf Basis von WLAN-Signalen stellt zwar die Grundlage zunehmend populärer Zusatzdienste (wie z. B. das Messen von Besucherströmen, Indoor Positionsbestimmung und Indoor -Navigation), birgt jedoch auch das Potenzial, die Privatheit und damit auch das Recht auf informationelle Selbstbestimmung zu beeinträchtigen.[86]

Neben gewerblichen Akteuren können auch öffentliche Akteure ein Interesse an einer weitergehenden Nutzung der Daten von WLAN-Nutzenden haben (siehe Abschnitt 2.4.1). So sind beispielweise Städte und Gemeinden zunehmend daran interessiert, Daten aus ihren öffentlichen WLAN-Hotspots als Grundlage ihrer Entscheidungen über Infrastrukturausbau einzusetzen.[87] In der Regel sind es allerdings eher die Anbieter privatwirtschaftlich betriebener öffentlicher WLANs bzw. von WLAN-Analysediensten, die auf Nutzerdaten zugreifen.

Seit dem 31. März 2016 müssen zudem die Betreiber von öffentlichen WLANs mit mehr als 10.000 Teilnehmenden (Cafés, Hotels, Bibliotheken usw. sind somit nicht betroffen) zudem alle erforderlichen organisatorischen und technischen Vorkehrungen treffen, um Ermittlungsbehörden eine Telekommunikationsüberwachung zu ermöglichen.[88] Von zivilgesellschaftlicher Seite ernteten derartige Maßnahmen, die zudem technisch relativ einfach zu umgehen sind, dahingehende Kritik, dass sie gegen schwere Straftaten wirkungslos seien und vermutlich eher für Aufklärungszwecke bei Urheberrechtsverstößen genutzt würden.[89] Dass eine großzügige Auslegung gesetzlicher Rahmenbedingungen insbesondere im Kontext von Überwachungsmaßnahmen stattfindet ist zudem ohnehin nicht erst seit den Snowden-Enthüllungen bekannt: So hatten etwa die Dresdner Polizeibehörden Anfang 2011 mithilfe einer – später gerichtlich für illegal befundenen – Funkzellenabfrage von Mobilfunkprovidern Zugriff auf ca. eine Million Datensätze mit Standortdaten und Kommunikationsmetadaten erhalten. Diese wurden jedoch nicht nur zur Aufklärung eines schweren Landfriedensbruchs, sondern auch bei Ermittlungen gegen Demonstrationsteilnehmer verwendet.[90] Ähnliches ist auch beim Tracking von WLAN-Nutzenden sowohl technisch möglich als auch angesichts vergleichbarer Vorfälle in der Vergangenheit real denkbar. Deutsche und europäische Anbieter sind hier immerhin an die rechtlichen Standards der EU gebunden, die europäischen und deutschen Bürgerinnen und Bürgern ein gewisses Maß an Rechtssicherheit gewähren. Anbieter von öffentlichen WLANs bzw. von WLAN-Analysediensten, die z. B. in den USA ansässig sind und in Europa agieren, können allerdings gemäß *USA PATRIOT Act* und *Communications Assistance for Law Enforcement Act* (CALEA) dazu verpflichtet werden, Strafermittlungsbehörden und Nachrichtendiensten weitreichenden Zugriff auf Daten ihrer im Ausland – also auch in Deutschland bzw. der EU – stehenden Server zu gewähren.[91] Dieser Zugriff steht zwar im Widerspruch zu europäischem und deutschem Datenschutzrecht, wurde jedoch in der Vergangenheit durch ein US-Bezirksgericht bestätigt.[92]

3.2.1 Welche Daten fallen bei der Nutzung öffentlicher WLANs an?

Angesichts der zurzeit noch hohen Preise für spezifische Überwachungssensoren in Innenräumen, stellen kostenfreie WLAN-Zugänge eine kostengünstige Alternative zur Erfassung von Nutzerdaten dar. Deshalb setzen viele Anbieter auf neue Kundenanalyse-, Kundenbindungs- und Marketingmöglichkeiten auf Basis von WLAN-Signalen. Ein Teil der dabei anfallenden Daten sind personenbeziehbar oder gar personenbezogen.[93]

Konto- und Registrierungsdaten

Je nach Konfiguration des Netzwerks kann die Angabe personenbezogener Daten wie einer E-Mail-Adresse, der Telefonnummer oder auch des Namens die Bedingung für die Benutzung eines WLANs darstellen. Internet Service Provider wie die Deutsche Telekom AG oder Unitymedia bieten ihren Kunden inzwischen deutschlandweit kostenfreien Zugang zu ihren öffentlichen WLANs. In solchen Fällen verfügen WLAN-Betreibende zusätzlich über Geburtsdatum, Geschlecht, Adresse und Zahlungsinformationen der Nutzenden.

Weil WLAN-Nutzende eine Neuanmeldung oft als lästiges Übel wahrnehmen, nutzen diese – sofern möglich – häufig die Möglichkeit einer Registrierung über Benutzerprofile auf sozialen Netzwerken von Facebook, Xing, Twitter usw. Dadurch entfällt die Neuregistrierung. Die vom WLAN-Betreiber benötigten Daten werden vom jeweiligen sozialen Netzwerk (z. B. Facebook) auf Anfrage bereitgestellt. So können WLAN-Betreibende aber auch Zugriff auf Details zum demografischen Hintergrund des Nutzenden erhalten. Dazu gehört u. a. das Alter, Geschlecht, Familienstand oder Religionszugehörigkeit. Im Gegenzug erhält der Betreiber des sozialen Netzwerks Informationen darüber, wann und mit welchem WLAN-Anbieter eine Nutzerin oder ein Nutzer interagiert hat.

Nutzungs- und Verhaltensdaten

Solange der WLAN-Adapter am mobilen Endgerät aktiviert bleibt, können die Bewegungen des Geräts bereits dann überwacht werden, wenn die Nutzenden (noch) gar nicht mit einem WLAN verbunden sind. Das betrifft also nicht nur Menschen, die bewusst ein WLAN-Angebot wahrnehmen indem sie ein Geschäft bzw. Einkaufszentrum betreten, sondern auch solche, die nur Schaufenster betrachten und auch jene, die lediglich daran vorbeilaufen. Wenn ein Geschäft betreten wird, können, abhängig davon, wie viele Router installiert sind, detaillierte Standortdaten mit einer Genauigkeit von weniger als einem Meter anfallen.[94] Einige private und auch öffentliche WLAN-Betreibende messen auf diese Weise Menschen- und Verkehrsflüsse in Städten bzw. im Stadtverkehr, an Flughäfen und auf öffentlichen Veranstaltungen.[95] Sofern ein Anbieter für Kundenanalyse Zugriff auf die Daten verschiedener Geschäfte hat, können Bewegungsprofile erzeugt werden. Dabei wird etwa ermittelt, wie häufig ein Kunde in ein Geschäft kommt, wie lange er sich dort aufhält, woher der Kunde in den Laden kommt und wohin er nach dem Verlassen des Ladens geht.[96]

Für eine noch detailliertere Kundenanalyse bieten Unternehmen zudem die Möglichkeit an, das Surfverhalten von Nutzerinnen und Nutzern (z. B. mittels Verknüpfung des WLAN-Trackings mit der Nutzung dedizierter Apps) zu verfolgen: Somit wird u. a. erfasst, welche Apps wie verwendet, welche Webseiten besucht und welche Produkte wo gekauft werden.[97]

Große US-amerikanische ISPs wie AT&T und Verizon haben bereits in der Vergangenheit demonstriert, dass sie die Internetnutzung ihrer Kunden analysieren. So war es Verizon möglich, das Kundenverhalten mithilfe eines Perma-Cookies zu verfolgen. Dabei wird jedem internetfähigen Gerät ein solcher Cookie individuell zugeordnet, der bei jeder Art von Internet-Traffic mit versendet wird. Er signalisiert Verizon, jeder aufgerufenen Internetseite und sogar Dritten, um welchen Nutzenden es sich handelt, sodass bspw. personalisierte Werbung angezeigt werden kann.[98]

Gerätespezifische Daten

Zu den gerätespezifischen Daten, die erfasst werden können, zählen die SSID-History, also die Namen aller Netzwerke, mit denen ein Nutzerendgerät jemals verbunden war, die MAC-Adresse sowohl des APs als auch des Nutzerendgeräts sowie dessen IP-Adresse.[99] Bei der Übermittlung der Probe Requests werden zudem sog. Information Elements (IE) (auch als sog. tagged parameters bezeichnet) übertragen. IEs sind Felder mit variabler Größe, in denen Details über unterstützte technische Fähigkeiten des Nutzergerätes angeben sind. So werden beispielweise Angaben über die unterstützen Übertragungsraten aus dem Feld mit der Bezeichnung *Supported Rates Information Element* kontinuierlich ausgesendet. Neben solchen Inhalten werden mit den Probe Requests außerdem (automatisch steigende) Sequenznummern übertragen. Die Angaben in IEs und die Sequenznummer in Probe Requests gelten als personenbeziehbar. Beide Datentypen können einem Gerät eindeutig zugeordnet und zu Trackingzwecken eingesetzt werden, ohne dass weitere Angaben über die MAC-Adresse benötigt werden.[100]

Ableitbare Daten

Je nach Vorhandensein und Wirtschaftlichkeit sind neben der einfachen Analyse des WLAN-Signals auch weitere Datenverknüpfungen möglich. So können WLAN-Daten mit Daten aus Überwachungskameras, Kreditkartentransaktionen, dem Browserverlauf und Konto- bzw. Registrierungsdaten verknüpft werden um einen noch tiefer gehenden Einblick in das Kundenverhalten zu erzielen (bspw. kann Stimmungsanalysesoftware eingesetzt werden um herauszufinden, welche Emotionen die Kunden an welchen Orten und zu welchem Zeitpunkt im Geschäft hatten).[101] Da die Persönlichkeit der Nutzenden ihr Nutzungsverhalten beeinflusst, ermöglicht die Auswertung von Nutzungs- und Verhaltensdaten auf Basis von Big Data-Analysetools bei einer ausreichend großen Datengrundlage umgekehrt mit einer gewissen Wahrscheinlichkeit Rückschlüsse auf Persönlichkeitsmerkmale und private Attribute der Kunden: Geschlecht, Alter, politische Einstellung, ethnischer Hintergrund, sexuelle Orientierung bzw. Vorlieben oder Hobbys.[102]

3.2.2 Privatheitsrisiken und Überwachungspotenziale

Aktuelle Initiativen zur Förderung des Ausbaus öffentlicher WLANs resultieren häufig in der Verbreitung von IT-Infrastrukturen, deren Sicherheit i. d. R. nicht in ausreichendem Maß sichergestellt wird. Kombiniert mit ökonomischen Anreizen, vielfältige Daten über WLAN-Nutzende systematisch zu erfassen und auszuwerten, birgt der Ausbau öffentlicher WLAN-Hotspots schwerwiegende Implikationen für die informationelle Selbstbestimmung der Betroffenen. Mögliche Privatheitsrisiken und Überwachungspotenziale können sich durch die Nutzung öffentlicher WLANs etwa in folgender Hinsicht ergeben.[103]

Intransparenz der Datenerfassung und -verarbeitung

Es ist davon auszugehen, dass das Bewusstsein auf Seiten der Nutzenden hinsichtlich der Privatheitsfolgen, die sich bei der Nutzung öffentlicher WLANs ergeben können, nur gering entwickelt ist.[104] So sind sich viele Menschen weder der Risiken des ständigen Tragens eines WLAN-fähigen Geräts bewusst noch können sie einschätzen, ob und wann Daten über sie und ihre Geräte erfasst und verarbeitet werden.[105] Gewerbliche als auch öffentliche Akteure nutzen den mangelhaften Kenntnisstand wiederum aus, um intrusive WLAN-Infrastrukturen aufzubauen und Daten über die Nutzerinnen und Nutzer WLAN-fähiger mobiler Endgeräte unautorisiert bzw. im Geheimen zu erfassen und zu bearbeiten – zumindest solange, bis derlei Praktiken zum Gegenstand medialer Berichterstattung und damit der öffentlichen Debatte werden.[106]

Zudem können auch öffentliche Stellen ein Interesse daran haben, auf Nutzerdaten zuzugreifen. Während ein solcher Zugriff einerseits zu Strafverfolgungszwecken auf

Grundlage geltender Gesetze erfolgen kann, kann andererseits nicht ausgeschlossen werden, dass unklare rechtliche Rahmenbedingungen Grauzonen schaffen, in deren Rahmen WLAN-Service-Provider Nutzerinnen- und Nutzerdaten an Sicherheitsbehörden und anderer staatliche Organe übertragen.[107] Dieser Aspekt gewinnt eine besondere Brisanz, wenn es beispielsweise um die Teilnahme an öffentlichen politischen Demonstrationen geht.[108]

Unklar bleibt auch, in welchem Verhältnis der Nutzen von Gewerbetreibenden und Datenanalyseunternehmen aus der Analyse von Nutzerdaten zu den Vorteilen steht, die den Nutzenden gewährt werden. Jedenfalls werfen die enormen Umsatzsteigerungen von Datenanalyseunternehmen dahingehende Zweifel *auf*, dass es sich hierbei um eine annähernd gerechte Aufteilung der Profite handelt, sofern die einzigen Vorteile für die Nutzenden darin bestehen, das WLAN kostenfrei nutzen zu können, gelegentliche Angebote zu erhalten und bessere Werbung angezeigt zu bekommen, während die Gegenseite – abhängig von Art und Umfang der Analyse, die von Anbieter zu Anbieter enorm variiert – durchaus auch hohe Profite erwirtschaften kann.[109]

Tracking und Profilbildung

Die intransparente Datenerhebung im Kontext neuartiger WLAN-basierter Infrastrukturen und Dienste stellt die Grundlage rechtlich fragwürdiger Profilbildung und versteckten Trackings dar. Derartige Profilbildung und Tracking werden auch ohne eine informierte Einwilligung der Betroffenen durchgeführt,[110] was Folgen für die Privatheit der Nutzerinnen und Nutzer hat: Die Betroffenen (sowohl jene Menschen, die das WLAN nutzen als auch alle Menschen, die lediglich ein WLAN-fähiges Gerät im Funkbereich, das Probe Requests aussendet, bei sich führen) verlieren damit Kontrolle über die eigenen Daten und werden somit bei der Wahrnehmung ihres Rechts auf informationelle Selbstbestimmung eingeschränkt.

Sofern zum Zwecke der Nutzung eines WLANs einer weitgehenden Datenerhebung zugestimmt wird, besteht die Möglichkeit der Profilbildung und des detaillierten On- und Offline-Trackings.[111] Die Verknüpfung von Standortdaten mit (Internet-)Nutzungs- und Verhaltensdaten sowie mit dem zugehörigen Benutzerprofil bei einem sozialen Netzwerk erlaubt die Erstellung eines detaillierten Nutzerprofils, auf das sowohl die Geschäftsinhaber als auch weitere Verarbeitende noch Jahre später zugreifen können.[112] Aber auch die Betreiber der Sozialen Netzwerke, mit deren Accounts die Nutzenden sich in ein WLAN einwählen, sind in der Lage, Informationen über die Nutzung des jeweils neuen WLANs zu erhalten.

Elektronische Überwachung und unabsichtliche Offenlegung vertraulicher Daten

Sobald WLAN-fähige mobile Endgeräte in den Funkbereich eines Zugangspunktes (WLAN-APs) eintreten, sammelt dieser nicht nur die MAC-Adresse, sondern auch Informationen darüber, wie sich Signale aus den Endgeräten durch die Luft bewegen und ob sie durch Hindernisse oder sonstige Störungen beeinflusst werden. Mit diesen Informationen können am Zugangspunkt Anpassungen vorgenommen werden, die dazu dienen, den Datenaustauch mit allen angeschlossenen Endgeräten stabiler und damit zuverlässiger zu gestalten. Allerdings können Zugangspunkte auch kompromittiert und WLAN-Daten zweckentfremdet werden, um etwa Menschen zu überwachen – z. T. in äußerst detaillierter Weise und oft ohne ihr Wissen oder Einverständnis.

So können Perma-Cookies dazu eingesetzt werden, die Online-Aktivitäten von WLAN-Nutzenden zu überwachen. Hotspot-Betreiber können unterschiedliche Gerätsignale erfassen und zum Zwecke der Lokalisierung WLAN-fähiger Endgeräte verwenden, bevor eine Internetverbindung über den WLAN-AP überhaupt hergestellt wurde. Neben gewerblichen Akteuren und kriminellen Hackern können sich auch global agierende Entitäten – wie z. B. der Geheimdienst eines anderen Staates –unberechtigt und unbemerkt Zugriff auf die in einer WLAN-Infrastruktur anfallenden Daten verschaffen, um

die Nutzerinnen und Nutzer WLAN-fähiger mobiler Endgeräte aus der Ferne gezielt zu überwachen. Zu diesem Zwecke werden in der Regel vorhandene Sicherheitslücken im WLAN-AP ausgenutzt.

Zudem können alle Akteure, die die WLAN-Signale von Nutzergeräten erfassen können, auch personenbedingte Änderungen im Funksignal feststellen. So können etwa wiederkehrende Muster in den Reflektionen des WLAN-Signals, die durch menschliche Körper verursacht werden, dazu verwendet werden, Personen (ihre Körpergröße, ihre Gangart usw.) zu identifizieren,[113] die Eingabe vertraulicher Daten (z. B. von Passwörtern und PIN-Codes) unbemerkt zu erfassen,[114] oder sogar Gesprächsinhalte aus der Analyse von Mund- und Lippenbewegungen heraus zu erkennen.[115]

Verlust oder Einschränkung der Entscheidungsfreiheit

Ereignisse in der Vergangenheit haben mehrfach gezeigt, dass WLAN-Tracking häufig ohne das Einverständnis der Nutzerinnen und Nutzer stattfindet. Die beteiligten Akteure verwiesen in solchen Fällen i. d. R. darauf, dass die grundsätzliche Möglichkeit des Opt-Out besteht, indem die Nutzenden ihr Smartphone oder den WLAN-Adapter ausschalten.[116]

Eine Einschränkung der Entscheidungsfreiheit kann etwa dann die Folge sein, wenn bei der Einholung des Einverständnisses sowohl eine umfangreiche Datenpreisgabe (etwa die Erlaubnis, die Online-Aktivitäten verfolgen zu dürfen), als auch die Erlaubnis, die Nutzerdaten mit anderen Daten abzugleichen sowie an Dritte weiterleiten zu dürfen, zur Bedingung für die Nutzung eines WLANs wird. Problematisch ist es zudem, wenn datenschutzbewusste Nutzerinnen und Nutzer aufgrund der weitreichenden Eingriffe in die Privatheit durch WLAN-Technologien bestimmte Areale meiden und damit ihre Bewegungsfreiheit eingeschränkt wird.

4 Regulativer Rahmen: Störerhaftung, Straf- und Datenschutzrecht

Regulatorische Rahmenbedingungen sind selten bloß Regelungen von Sachverhalten auf Grundlage unstrittiger Fakten. Vielmehr gehen ihnen gesellschaftliche Auseinandersetzungen voraus, deren Resultat rechtliche Regelungen darstellen. Diese sind dann sowohl Ausdruck der Kräfteverhältnisse der im jeweiligen Politikfeld aktiven Akteure als auch ein Kompromiss zwischen den konfligierenden Akteursinteressen auf Grundlage diverser Pfadabhängigkeiten – z. B. von den bislang geltenden Gesetzen, institutionellen Rahmenbedingungen, Verarbeitung technischen Wissens etc. Ein besseres Verständnis des politischen Prozesses erlaubt es daher auch vorsichtige Aussagen darüber zu treffen, wie ein Politikfeld sich über den Status Quo hinaus entwickeln mag.

Gerade das politische Nischenthema um das Haftungsrecht im Kontext öffentlicher WLANs hat in den vergangenen Jahren sowohl einen Bedeutungszugewinn erhalten, als auch einen konfliktbeladenen politischen Prozess in Gang gesetzt, der mit aller Wahrscheinlichkeit auch weiterhin die Politik beschäftigen wird. Einleitend soll im Folgenden zunächst die politische Debatte skizziert (4.1) sowie im Anschluss der gegenwärtige rechtliche Status Quo im Detail vorgestellt werden (4.2).

Das Thema öffentlicher WLANs betrifft allerdings nicht nur das Haftungsrecht. Im Kontext der Verwundbarkeit öffentlicher WLANs gegenüber Angriffen stellt sich auch die Frage, welche Handhabe das Strafgesetzbuch nach derzeitiger Rechtslage gegenüber derartigen Angreifern gewährt. Eine solche Untersuchung ist Gegenstand von Abschnitt 4.3.

In Abschnitt 4.4 werden übergreifende datenschutzrechtliche Fragen aufgegriffen: Denn datenschutzrechtliche Regelungen greifen nicht allein beim Betrieb öffentlicher WLANs, auch die haftungsrechtlichen Probleme haben Auswirkungen auf die Belange des Datenschutzes.

4.1 Gesellschaftliche Auseinandersetzungen um öffentliche WLANs

Sowohl von Seiten der Zivilgesellschaft[117] als auch von Teilen der Wirtschaft[118], insbesondere den Verbänden der Internetwirtschaft (allen voran Eco und BITKOM), wurden unter Verweis auf die wirtschaftlichen und sozialen Chancen seit Jahren Forderungen nach einer rechtlichen Klarstellung im Bereich der sowohl gewerblichen als auch privaten Bereitstellung von WLAN-Hotspots gestellt. Auf der anderen Seite gingen Rechteinhaber (Film-, Musik, Entertainment-Software- und Verlagswirtschaft und deren Vertreter wie GEMA und VG Wort) und Kanzleien, die im Auftrag von Urheberrechtsinhabern Unterlassungsansprüche und gerichtliche wie außergerichtliche Kosten geltend machen, gegen eine Gleichstellung „nicht-traditioneller" Provider vor. Den Vertretern dieser Urheberrechtsinteressen zufolge hätte eine Lockerung der Gesetzeslage eine Verschlechterung der ohnehin schwierigen wirtschaftlichen Lage der Kreativwirtschaft zur Folge.[119] Kritiker dagegen sehen in dieser Argumentation eine Verteidigung des sehr erfolgreichen Geschäftsmodells der Abmahnindustrie, der damit die rechtliche Grundlage entzogen würde.[120]

Aufgrund des steigenden Drucks kündigte die Regierungskoalition aus CDU/CSU und SPD schließlich im Koalitionsvertrag von 2013 – öffentliche WLANs als Chance auf Innovation, Fortschritt und neue Beschäftigung begreifend – an, dass die Grundlagen für Nutzende und Anbieter öffentlicher WLANs geschaffen werden sollen, indem z. B. eine Verbesserung der Rechtssicherheit für WLAN-Betreibende mithilfe einer Klarstellung der

Haftungsregelungen erfolgt. Zugleich wurde eine Aufklärung von Bürgerinnen und Bürgern über die Gefahren bei einer Nutzung öffentlicher WLAN-Dienste angekündigt.[121]

Die Ankündigungen des Koalitionsvertrags wurden im Rahmen der im August 2014 veröffentlichten Digitalen Agenda noch einmal bekräftigt und spezifiziert: So wurden zu den Anbietern im öffentlichen Bereich, die grundsätzlich nicht für Rechtsverletzungen ihrer Kundschaft haften sollen, *beispielsweise Flughäfen, Hotels und Cafés* gezählt.[122] Zudem wurde betont, dass darauf geachtet werde, dass die IT-Sicherheit gewahrt bleibt und durch ein Ende der Störerhaftung keine neuen Einfallstore für anonyme Kriminalität entstehen. Das Fehlen von öffentlichen WLANs, die von Bürgerinnen und Bürgern ohne kommerzielle Interessen betrieben werden, in der Aufzählung, führte im Anschluss zu Kritik von Seiten zivilgesellschaftlicher Akteure.[123]

Zuvor war bereits bekannt geworden, dass Bundeswirtschaftsminister Gabriel im August 2014 einen ersten Gesetzentwurf in die Ressortabstimmung geben würde.[124] Allerdings konnten sich die Regierungsfraktionen zunächst nicht auf eine gemeinsame Linie einigen: Streitpunkte bestanden sowohl im Hinblick darauf, was unter Sorgfaltspflichten bzw. „zumutbaren Maßnahmen" zur Vermeidung von Rechtsverletzungen zu verstehen ist, als auch dahingehend, wie weit eine Freistellung von der Störerhaftung für die verschiedenen Arten von WLAN-Betreibenden greifen sollte, um möglichst vielen Betreibern Rechtssicherheit zu bieten, während zugleich die Verwertungsinteressen von Rechteinhabern berücksichtigt werden.[125] Der parteipolitische Zwist war auch auf Landesebene zu spüren: Die SPD-geführten Bundesländer Nordrhein-Westfalen und Bremen forderten ebenfalls die Abschaffung der Störerhaftung.[126]

In der Zwischenzeit hatten bereits Abgeordnete der Grünen und der Linken 2013 im November 2014 einen Gesetzentwurf der zivilgesellschaftlichen Nichtregierungsorganisation *Digitale Gesellschaft e. V.* zur Störerhaftung bei öffentlichen WLANs eingebracht.[127] Auf Empfehlung des federführenden Wirtschaftsausschusses hin wurden beide Gesetze mit der Stimmenmehrheit der Regierungskoalition abgelehnt.[128] Während die CDU/CSU-Fraktion im Wirtschaftsausschuss insbesondere auf den im Entwurf fehlenden Sicherheitsaspekt rekurrierte, verwies die SPD-Fraktion in ihrer Ablehnung und trotz der generellen Befürwortung der Zielrichtung des Entwurfs auf den anhaltenden Klärungsbedarf innerhalb der Koalition.[129]

Ein erster nicht-abgestimmter Referentenentwurf zu einer Änderung des TMG wurde schließlich Ende Februar 2015 bekannt. Darin hieß es zunächst, dass „*alle anderen Diensteanbieter, die den Internetzugang zur Verfügung stellen, nur dann nicht als Störer auf Unterlassen haften, wenn sie zumutbare Maßnahmen […] getroffen haben und den Namen des Nutzers kennen.*"[130]

Mitte März 2015 wurde der zweite Referentenentwurf aus dem SPD-geführten Wirtschaftsministerium veröffentlicht. Dieser wurde als weitgehendes Entgegenkommen gegenüber den Verwertungsinteressen der Rechteinhaber-Lobby gedeutet, da deutlich höhere Anforderungen an Sicherungsmaßnahmen beim privaten WLAN-Betrieb gestellt wurden als bei gewerblichen oder öffentlich betriebenen WLAN-Hotspots. Als – im Anschluss von zivilgesellschaftlicher Seite her enorm kritisierte – Begründung dazu wurde aufgeführt, dass die Möglichkeit Straftaten (etwa das Verbreiten von Kinderpornografie oder Urheberrechtsverletzungen) zu begehen, in Privaträumen erheblich größer sei als im öffentlichen Raum.[131] Während die Koalition der Rechteinhaber für eine weitere Verschärfung des Inhalts (z. B. im Hinblick auf die Aufsichtspflichten der WLAN-Betreibenden) plädierte[132], zeigten die Folgemonate, dass die Kritik aus Zivilgesellschaft[133] und Internetwirtschaft[134] grundsätzlich sowohl auf Seiten der EU-Kommission als auch beim Bundesrat Anklang fand.

Zunächst hatte die Bundesregierung den zweiten Gesetzentwurf auf die massive Kritik hin überarbeitet (z. B. dahingehend, dass private WLAN-Anbieter gewerblichen und öffentlichen Anbietern rechtlich gleichgestellt werden sollten und indem eine Reduzie-

rung der vorgeschriebenen Sicherheitsmaßnahmen vorgesehen wurde) und zwecks Notifizierung an die Europäische Kommission übergeben. Die Kommission bemängelte in einem internen Schreiben an die Bundesregierung, dass der Entwurf mit dem Europarecht nicht vereinbar sei. Insbesondere würden die vorgesehenen Regelungen weder mit den Vorgaben der europäischen E-Commerce-Richtlinie im Einklang stehen noch seien sie mit den europäischen Grundrechten auf freie Meinungsäußerung und unternehmerische Freiheit vereinbar.[135] Der Bundesrat schloss sich derweil den haftungs- und europarechtlichen Bedenken der zivilgesellschaftlichen Akteure[136] und der EU-Kommission an und forderte eine Ausweitung der Haftungsprivilegien auf private, nicht-gewerbliche Anbieter.[137]

Nach jahrelangem Tauziehen um die Störerhaftung wurde der immer noch höchst umstrittene Gesetzentwurf[138] mit zwei Änderungsanträgen und einem Erschließungsantrag am 2. Juni 2016 vom Bundestag verabschiedet. Obwohl die Entscheidung des EuGH zur Störerhaftung beim Betrieb offener WLANs[139] (siehe 4.2.2) absehbar war, hatte die Bundesregierung nach den Schlussanträgen des EuGH-Generalanwalts im März 2016 regelrecht darauf gedrängt, sich auf eine gesetzliche Regelung der Störerhaftung zu einigen. Auch wenn die Gründe für dieses Vorgehen an dieser Stelle nicht abschließend diskutiert werden können, so kann davon ausgegangen werden, dass die immer näher rückende Bundestagswahl im Herbst 2017 sowie das Interesse der Bundesregierung daran, Tatsachen zu schaffen, eine ausschlaggebende Rolle gespielt haben.

Der in der Koalition abgestimmte Kompromiss wurde mit den Stimmen der CDU, CSU und SPD angenommen. Während die große Koalition die Neuregelung der Störerhaftung für tragfähig hielt, indem die WLAN-Anbieter bei rechtswidrigen Handlungen Dritter nicht auf Zahlung von Schadensersatz und Zahlung von Abmahn- und Gerichtskosten verurteilt werden können und die Haftungsbeschränkung nicht dem Erlass einer gerichtlichen Anordnung auf Unterlassung entgegensteht, stimmten Linke und Grüne gegen die Gesetzesänderung. Sie betonten, dass auch weiterhin Abmahnrisiken für die WLAN-Anbieter bleiben würden und Rechtssicherheit damit nicht erreicht werden kann.[140]

Am 27. Juli 2016 – zwei Monate vor der Entscheidung des EuGH zur Haftung von Anbietern beim Betrieb öffentlicher WLANs – ist das Zweite Gesetz zur Änderung des Telemediengesetzes[141] in Kraft getreten, das u. a. das Ziel verfolgt, für WLAN-Anbieter mehr Rechtssicherheit zu schaffen und damit zum Ausbau öffentlicher WLANs beizutragen.[142] Der in § 8 TMG neu eingefügte Absatz 3 bestimmt jedoch nur, dass auch Anbieter von WLAN-Zugängen Access-Provider (wie z. B. Vodafone GmbH und Telekom Deutschland GmbH) sind und für diese auch die Bestimmungen des § 8 TMG gelten. Wichtige Erwägungen, die für die Klärung der WLAN-Störerhaftung von großer Relevanz sind, finden sich jedoch lediglich in der – für Gerichte nicht-bindenden – Gesetzesbegründung wieder. Kritisiert wurde vor allem, dass auch nach der Änderung des § 8 TMG die Gefahr vor Schadensersatzansprüchen und Abmahnungen nicht völlig ausgeräumt wurde.[143] Umso mehr wurde die Entscheidung des EuGH erwartet, die Klarheit für die Anbieter öffentlicher WLANs bringen sollte.[144]

Der EuGH urteilte schließlich am 15. September 2016 dahingehend, dass (gewerbliche) Anbieter sich nicht für Urheberrechtsverletzungen der Nutzenden beim Betrieb offener WLANs verantworten müssen.[145] Der EuGH stellt damit zwar klar, dass Schadensersatzansprüche nicht erhoben werden können und die WLAN-Anbieter die damit verbundene Abmahn- und Gerichtskosten nicht zu tragen haben. Allerdings können die WLAN-Anbieter von nationalen Gerichten oder innerstaatlichen Behörden dazu aufgefordert werden, angemessene und verhältnismäßige Maßnahmen zur Verhinderung weiterer Rechtsverstöße zu ergreifen.

4.2 Haftungsrecht – Störerhaftung beim Betrieb öffentlicher WLANs

Nachdem die Entwicklung hin zu den aktuellen rechtlichen Rahmenbedingungen im Bereich des Haftungsrechts erläutert wurde, sollen diese Regelungen nun im Detail diskutiert werden. Im Ergebnis wird sich zeigen, dass trotz der jüngsten Gesetzesanpassungen für die Anbieter öffentlicher WLANs auch weiterhin nur geringe Rechtssicherheit herrscht.

4.2.1 Störerhaftung und die bisherige Rechtslage beim Betrieb öffentlicher WLANs

Begriff der Störerhaftung im Allgemeinen

Störer sind Personen, die selbst weder Täter noch Teilnehmende sind, aber mit ihrem Handeln in irgendeiner Weise – willentlich oder adäquat kausal – dazu beitragen, dass ein geschütztes Rechtsgut verletzt wird.[146] Dieser aus dem Wettbewerbsrecht stammende Begriff des Störers geht von einem Ansatz aus und ist verschuldensunabhängig.[147] Damit ist gemeint, dass es weder auf Vorsatz noch auf Fahrlässigkeit des Störers ankommt: Dieser muss auch dann haften, wenn kein Verschulden und keine Kenntnis der beeinträchtigenden Handlung vorliegen.

Störerhaftung beim Betrieb offener WLANs

Im Rahmen der Vorschriften zur Verantwortlichkeit von Telemedienanbietern ist die Einordung der Störerhaftung von WLAN-Anbietern sehr umstritten. Die Ermittlung eines Schädigers oder Täters bei Rechtsverletzungen ist beim Betrieb offener WLANs sehr schwierig. Kann derjenige, der die Rechtsverletzung begangen hat, nicht festgestellt werden, bleibt dem Geschädigten nur, den WLAN-Anbieter zu belangen.[148] Als Störer haften bei Rechtsverstößen Dritter in analoger Anwendung von §§ 823, 1004 BGB (Bürgerliches Gesetzbuch) diejenigen, die adäquat kausal – bei mittelbarer Störerhaftung ohne selbst Täter oder Teilnehmende zu sein – an der Herbeiführung oder Aufrechterhaltung einer Rechtsverletzung mitgewirkt haben, selbst wenn diese kein eigenes Verschulden trifft.[149] Bei WLAN-Anbietern liegt die adäquat-kausale Mitwirkung an der Rechtsverletzung zumindest in der Vermittlung des Zugangs zum Internet. Sie setzen eine Ursache, indem sie ihr WLAN einem Schädiger öffnen und damit zur Begehung einer Rechtsverletzung beitragen.

Haftungsprivilegierung nach § 8 TMG

Voraussetzungen

Die Haftungsprivilegierung für Access- oder Zugangsprovider, die für ihre Kundschaft den Zugang zu einem Kommunikationsnetz herstellen, ist in § 8 TMG normiert. Gemäß § 8 Abs. 1 TMG sind solche Anbieter nicht für die durchgeleiteten Informationen durch ihre Netze verantwortlich, sofern sie die Übermittlung fremder Informationen nicht veranlasst haben, den Adressaten der übermittelten Informationen und die übermittelten Informationen selbst nicht ausgewählt oder verändert haben.[150] Access Provider (wie z. B. Telekom Deutschland GmbH und Vodafone GmbH) sind von der Haftung weitgehend ausgenommen und genießen damit das sogenannte „Providerprivileg". Die Begründung dafür folgt der Auffassung, dass durch die Netze der Access Provider eine unüberschaubare Masse an Informationen fließt, die von diesen nicht kontrolliert werden kann. Da den Access Providern, da sie lediglich die Daten der Nutzenden übermitteln, eine neutrale Vermittlerposition zukommt, wirken sie an der Rechtsverletzung nicht mit und werden daher von der Verantwortlichkeit ausgeschlossen.[151]

Persönlicher Anwendungsbereich und die Entscheidung des Bundesgerichtshofs „Sommer unseres Lebens"

Trotz einer sehr weit gefassten Regelung des § 8 TMG ist nicht einheitlich entschieden worden, für welche Anbieter das Providerprivileg, das zur Haftungsfreistellung führt, gilt und unter welchen Voraussetzungen dieses zur Anwendung kommt.[152] Während die Gerichte ohne weiteres das Providerprivileg des § 8 Abs. 1 TMG bei den klassischen Providern wie z. B. Telekom Deutschland GmbH oder Unitymedia GmbH, deren Schwerpunkt in der Vermarktung von Internetzugängen liegt, ohne weiteres annehmen, bestehen große Rechtsunsicherheiten, ob auch WLAN-Anbieter unter die Haftungsbeschränkungen des § 8 Abs. 1 TMG fallen.[153] Auch wenn nach herrschender Meinung das Angebot eines WLAN-Zugangs in den sachlichen Anwendungsbereich des § 8 TMG fällt, ist bislang nicht geklärt worden, ob auch die „Nebenbei-Provider" von dem persönlichen Anwendungsbereich des § 8 TMG umfasst sind.[154] Zu den „Nebenbei-Providern" zählen z. B. Hotel-, Café- und Restaurantbetreiber, die ihren Gästen einen WLAN-Zugang anbieten, aber auch Schulen, Jugendeinrichtungen, Initiativen wie „Freifunk" oder auch Privatpersonen, die ihren häuslichen WLAN-Zugang nicht mit einem Passwort versehen.[155] Weder Art. 12 E-Commerce-RL 2000/31/EG noch der darauf beruhende § 8 TMG sahen eine Differenzierung zwischen den Anbietern vor.[156]

Der Bundesgerichtshof (BGH) hatte zwar in dem Urteil „Sommer unseres Lebens"[157] vom 12. Mai 2010 eine Grundlagenentscheidung zum Thema Filesharing[158] und WLAN-Betrieb im privaten Bereich gefällt. Allerdings befasst sich das Gericht weder damit, ob die WLAN-Anbieter den Access Providern gleichgestellt sind und somit das „Providerprivileg" des § 8 TMG auf sie anwendbar ist, noch klärt es die Frage, ob dieses Privileg auf die gewerblichen und die privaten WLAN-Anbieter Anwendung findet.[159]

Die Entscheidung des BGH „Sommer unseres Lebens" stellt lediglich die Grundzüge der Störerhaftung für WLAN-Anschlussinhaber bei Rechtsverletzungen durch Dritte dar.[160] Das Gericht betont, dass der Betrieb eines unzureichend gesicherten WLAN-Anschlusses adäquat-kausal für Verletzungen des Urheberrechts ist, die Dritte ohne Kenntnis des Anschlussinhabers begehen. Das Gericht bejaht die Pflicht von WLAN-Anbietern zur Unterlassung, lehnt allerdings die Störerhaftung für den Schadensersatzanspruch ausdrücklich ab. Das Gericht geht in seiner Entscheidung nur darauf ein, welchen Sorgfaltspflichten ein privater WLAN-Anbieter nachgehen muss, um sich nicht nach den Grundsätzen der Störerhaftung bei rechtswidrigen Handlungen Dritter verantworten zu müssen. Private WLAN-Anbieter trifft nach dieser Entscheidung des Gerichts die Pflicht, ihren Zugang zum WLAN durch marktübliche Sicherheitsstandards, wie z. B. individuelle Passwörter, zu schützen.

Sachlicher Anwendungsbereich

Die Privilegierung nach § 8 TMG umfasst weder zivilrechtliche Anspruchsgrundlagen, noch strafrechtliche Tatbestände oder Ermächtigungsgrundlagen im öffentlich-rechtlichen Bereich. Die Verantwortlichkeit ergibt sich aus den allgemeinen Grundsätzen des jeweiligen spezifischen Haftungsrechts (z. B. Deliktsrecht oder Urheberrecht).[161]

Zu beachten ist allerdings, dass die Privilegierung der Diensteanbieter im Sinne des § 8 TMG durch § 7 Abs. 2 Satz 2 TMG eingeschränkt wird.[162] Dieser ordnet an, dass Verpflichtungen der Diensteanbieter zu Sperrung oder Entfernung von Informationen nach den allgemeinen Grundsätzen unberührt bleiben. Diese Vorschrift stellt jedoch keine eigenständige Rechtsgrundlage dar. Sind also Informationen zu sperren oder zu entfernen, bedarf es einer allgemein zivilrechtlichen oder öffentlich-rechtlichen Anspruchsgrundlage (z. B. §§ 823, 1004 BGB, § 97 Abs. 1 Satz 1 UrhG).[163]

4.2.2 Entscheidung des EuGH zur Anbieterhaftung beim Betrieb eines offenen WLANs

Der EuGH hatte darüber zu entscheiden, ob und in welchem Umfang Gewerbetreibende für Urheberrechtsverletzungen haften, wenn sie ihnen im Rahmen ihrer wirtschaftlichen Tätigkeit einen unentgeltlichen offenen WLAN-Zugang zur Verfügung stellen und über diesen Rechtsverletzungen begangen werden. Der EuGH war bei seiner am 15. September 2016 verkündeten Entscheidung den Schlussanträgen des Generalanwalts Maciej Szpunar zum Teil nicht gefolgt.[164]

Anwendungsbereich der E-Commerce-Richtlinie

Der EuGH stellt zunächst fest, dass WLAN-Anbieter, die ihr Netz der Öffentlichkeit unentgeltlich zur Verfügung stellen, auch einen sog. *Dienst der Informationsgesellschaft* im Sinne von Art. 12 Abs. 1 E-Commerce-RL erbringen, sofern diese Leistung zu Werbezwecken für die vom Anbieter verkauften Güter oder angebotenen Dienstleistungen erbracht wird.[165]

Abschließende Anwendung des Art. 12 E-Commerce-RL

Des Weiteren betont der EuGH, dass für Anbieter, die ihr WLAN der Öffentlichkeit zur Verfügung stellen, ausschließlich Art. 12 E-Commerce-RL gilt. Das Gericht stellt klar, dass WLAN-Anbieter, die lediglich einen Zugang zu einem Kommunikationsnetz vermitteln und Anbieter, die Informationen auf ihrer Webseite speichern (Host-Provider), im Hinblick auf die in Art. 14 Abs. 1 E-Commerce-RL normierte Voraussetzung sich nicht in der gleichen Lage befinden. Im Gegensatz zu Host-Providern haben Diensteanbieter, die die übermittelten Informationen nicht kontrollieren können, häufig nicht die Möglichkeit, zu einem späteren Zeitpunkt tätig zu werden, um bestimmte Informationen zu entfernen oder den Zugang zu ihnen zu sperren. Demzufolge sei die Anwendbarkeit des Art. 14 Abs. 1 E-Commerce-RL im Rahmen des Art. 12 E-Commerce-RL zu verneinen.[166] Darüber hinaus stellt der EuGH fest, dass Art. 12 Abs. 1 i. V. m. Art. 2 lit. b E-Commerce-RL für einen solchen Dienst ausdrücklich nur die dort genannten Anforderungen vorsieht. Bei Diensteanbietern, die einen Zugang zu einem Kommunikationsnetz vermitteln, muss es sich lediglich um eine natürliche oder juristische Person handeln, die einen Dienst der Informationsgesellschaft anbietet.[167] Demnach sei Art. 12 Abs. 1 i. V. m. Art 2 lit. b E-Commerce-RL dahingehend auszulegen, dass diese Voraussetzungen abschließend sind und daher keine weiteren Voraussetzungen vom Diensteanbieter verlangt werden können.[168]

Reichweite der Ansprüche aus Art. 12 E-Commerce-RL

Des Weiteren führt der EuGH aus, dass derjenige, der durch eine Verletzung seiner Urheberrechte geschädigt worden ist, vom WLAN-Anbieter, dessen Dienst zur Begehung einer Urheberrechtsverletzung genutzt wurde, keine Ansprüche auf Unterlassung, Schadensersatz sowie Zahlung von Abmahn- und Gerichtskosten geltend machen kann, wenn drei Voraussetzungen erfüllt sind: Der Diensteanbieter hat die Übermittlung nicht veranlasst; hat die Adressaten, die die Informationen übermitteln, nicht ausgewählt; und hat die übermittelten Informationen nicht verändert.

Ferner trifft das Gericht die Aussage, dass Art. 12 Abs. 2 E-Commerce-RL die Möglichkeit unberührt lässt, dass ein Gericht oder eine Verwaltungsbehörde vom Diensteanbieter verlangen kann, die Rechtsverletzung abzustellen oder zu verhindern. In dem Zusammenhang führt der EuGH aus, dass Art. 12 Abs. 1 E-Commerce-RL keinesfalls ausschließt, dass beim Bestehen eines Unterlassungsanspruchs der Rechteinhaber vom Diensteanbieter die Erstattung der dabei anfallenden Abmahn- und Gerichtskosten verlangen kann.[169]

Maßnahmen zur Verhinderung weiterer Rechtsverstöße

Darüber hinaus teilt der EuGH mit, dass dem Diensteanbieter die Pflicht auferlegt werden kann, technische Maßnahmen zu ergreifen, um weitere Rechtsverletzungen abzustellen oder zu verhindern. Dabei betont das Gericht jedoch, dass die Überprüfung sämtlicher, durch einen WLAN-Anschluss übermittelter, Informationen Art. 15 Abs. 1 E-Commerce-RL zuwiderläuft.[170] Die Forderung nach einer vollständigen Stilllegung des Internetanschlusses wird für unzumutbar gehalten und scheidet ebenfalls aus.[171] Allerdings sieht der EuGH die Sicherung des Internetanschlusses mit einem Passwort als geeignet an, um ein Gleichgewicht zwischen den kollidierenden Grundrechten (Recht am geistigen Eigentum vs. Recht auf unternehmerische Freiheit und Recht der Nutzenden auf Informationsfreiheit) herzustellen.[172] Eine solche Maßnahme sei nach Ansicht des EuGH dazu geeignet, Nutzende von der Verletzung des Urheber- oder eines verwandten Schutzrechts abzuhalten. Schließlich betont das Gericht, dass es erforderlich ist, die WLAN-Nutzenden vor der Passwortausgabe zu identifizieren, damit sie im Internet nicht anonym handeln können.[173]

In diesem Punkt vertrat der EuGH jedoch eine andere Meinung als der EuGH-Generalanwalt, der in seinen Schlussanträgen der Auffassung war, dass Diensteanbieter zwar mittels einer gerichtlichen Anordnung dazu verpflichtet werden können, beanstandete Rechtsverletzungen zu verhindern oder zu beenden, eine Verschlüsselung und Passwortsicherung des WLANs jedoch ungeeignet und unverhältnismäßig sei.[174]

4.2.3 Regelungsumfang des § 8 Abs. 3 TMG

Der in § 8 TMG neu eingefügte Absatz 3 bestimmt, dass auch WLAN-Anbieter Access-Provider sind, womit auf sie die Bestimmungen des § 8 TMG anwendbar sind. Da § 8 Abs. 3 TMG jedoch keine Einschränkung im Hinblick auf eine bestimmte Gruppe von WLAN-Anbietern macht, werden sowohl gewerbliche als auch private WLAN-Anbieter von der Regelung umfasst. Die Regelung der Anbieterhaftung beim Betrieb offener WLANs hat allerdings keinen direkten Eingang ins Gesetz gefunden und findet sich lediglich in der Gesetzesbegründung. Aus dieser geht hervor, dass die Haftung der WLAN-Anbieter für rechtswidriges Verhalten der Nutzenden sich nicht nur auf die straf-, verwaltungs- und zivilrechtliche Haftung erstreckt, sondern auch auf die unmittelbare und mittelbare Haftung für rechtswidrige Handlungen Dritter. Somit umfasst die Haftungsprivilegierung der WLAN-Anbieter gemäß § 8 Abs. 1 und 2 TMG auch die Störerhaftung.[175]

Demzufolge können die WLAN-Anbieter weder zur Zahlung von Schadensersatz noch zum Tragen von Abmahn- und Gerichtskosten verurteilt werden, die im Zusammenhang mit einer (Urheber-)Rechtsverletzung stehen, die von einem Dritten über das WLAN des Anbieters begangen worden ist. Allerdings werden der Haftungsbefreiung der WLAN-Anbieter in der Gesetzesbegründung auch Grenzen gesetzt indem klargestellt wird, dass die Haftungsbeschränkung dem Erlass einer gerichtlichen Anordnung auf einer entsprechenden Gesetzesgrundlage nicht entgegensteht. Eine gerichtliche Anordnung muss wirksam und verhältnismäßig sowie darauf gerichtet sein, eine bestimmte Rechtsverletzung abzustellen oder zu verhindern, um ein angemessenes Gleichgewicht zwischen den Grundrechten zu wahren.[176] Des Weiteren ist der Gesetzesbegründung zu entnehmen, dass es rechtlich unzulässig ist, WLAN-Anbietern die Pflicht aufzuerlegen, den Internetzugang stillzulegen, das WLAN zu verschlüsseln bzw. mit einem Passwort zu schützen oder die Kommunikation der Nutzenden zu überwachen, damit diese einer gerichtlichen Anordnung nachkommen können,[177] so wie es der EuGH-Generalanwalt in seinen Schlussanträgen gefordert hat. [178]

4.2.4 Auswirkungen des EuGH-Urteils und des § 8 Abs.3 TMG auf die WLAN-Anbieter

Die Bundesregierung hat im Prozess der Änderung des Telemediengesetzes oftmals verkündet, dass die Änderung des § 8 TMG mehr Rechtssicherheit für WLAN-Anbieter

schaffen und die Nutzung und Verbreitung von öffentlichen WLANs erleichtern soll. Allerdings waren auch nach der Novellierung des § 8 TMG weiterhin viele rechtliche Fragen für die WLAN-Anbieter offengeblieben. Daher erhofften sich viele, dass die Entscheidung des EuGH die Rechtslage der Anbieter beim offenen WLAN-Betrieb endgültig klären und die bestehenden Unklarheiten im Hinblick auf die Störerhaftung beseitigen würde. Im Folgenden wird aufgezeigt, welche Auswirkungen auf die WLAN-Anbieter nach dem EuGH-Urteil und der Gesetzesänderung zu erwarten sind.

Differenzierung zwischen gewerblichen und privaten WLAN-Anbietern

Das Urteil des EuGH bezieht sich nur auf gewerbliche Anbieter, die ihr WLAN der Öffentlichkeit zur Verfügung stellen. Diese werden als „Diensteanbieter" im Sinne des Art. 12 E-Commerce-RL bzw. § 8 TMG (Access-Provider) betrachtet. In diesem Punkt deckt sich die Entscheidung des EuGH mit der Regelung des § 8 Abs. 3 TMG,[179] nach der WLAN-Anbieter Diensteanbieter im Sinne des § 8 TMG sind.

Zum privaten WLAN-Betrieb äußert sich der EuGH allerdings nicht, da sie von der Vorlagefrage an das Gericht nicht betroffen war. Demzufolge ist nur für die gewerblichen WLAN-Anbieter klargestellt worden, dass auf sie Art. 12 Abs. 1 E-Commerce-RL Anwendung findet.[180]

Für die privaten WLAN-Anbieter hat dies zur Folge, dass sie dem persönlichen Anwendungsbereich der E-Commerce-RL nicht unterfallen. Auf diese findet somit die Regelung des § 8 Abs. 3 TMG Anwendung, die keine Unterscheidung zwischen gewerblichen und privaten WLAN-Anbietern vorsieht.[181]

Auch wenn zunächst unklar ist, ob und in welchem Umfang die Entscheidung des EuGH Anwendung auf private WLAN-Anbieter findet, ist zu konstatieren, dass private WLAN-Anbieter aufgrund des Gleichbehandlungsgrundsatzes des Art. 3 GG nicht schlechter als gewerbliche WLAN-Anbieter gestellt werden dürfen.[182] Dies hätte für die privaten WLAN-Anbieter allerdings zur Folge, dass sie zwar vor Schadensersatzansprüchen der Rechteinhaber und den mit ihnen einhergehenden Abmahn- und Gerichtskosten bei Urheberrechtsverletzungen durch Dritte geschützt wären. Allerdings ist die Tatsache nicht zu vernachlässigen, dass sie damit zum einen der Gefahr gerichtlicher oder behördlicher Anordnungen mit Festsetzung von technischen Maßnahmen zur Verhinderung weiterer Rechtsverstöße ausgesetzt wären. Zum anderen könnten den privaten WLAN-Anbietern auch die damit verbundenen Abmahn- und Gerichtskosten in Rechnung gestellt werden.

Beseitigung von Unterlassungsansprüchen nach nationalem Recht?

Im Zusammenhang mit der Änderung des § 8 TMG wurde oftmals kritisiert, dass die von der Bundesregierung angestrebte Rechtssicherheit beim WLAN-Betrieb nicht gewährleistet werden kann, da Unterlassungsansprüche mittels einer gerichtlichen Anordnung nach § 8 Abs. 3 TMG auch weiterhin möglich sind.

Der EuGH stellt in seiner Entscheidung fest, dass (gewerbliche) WLAN-Anbieter zwar das Haftungsprivileg weitgehend genießen, Geschädigte (Rechteinhaber) aber dennoch von einem Gericht oder einer innerstaatlichen Behörde verlangen können, eine Anordnung zu erlassen, um eine Rechtsverletzung abzustellen oder zu verhindern. Dies hat zur Folge, dass der EuGH dem nationalen Gesetzgeber zwar nicht ausdrücklich den Erlass von behördlichen oder gerichtlichen Anordnungen vorschreibt, diese jedoch legitimiert. Fraglich ist allerdings, ob der deutsche Gesetzgeber die Unterlassungsansprüche gegen die WLAN-Anbieter auch vollständig ausschließen kann, wie es von den Gegnern der Störerhaftung schon lange gefordert wird.

Die „völlige Abschaffung" der Störerhaftung durch den nationalen Gesetzgeber ist allerdings nicht ohne Weiteres umsetzbar, denn die dabei zu beachtenden europarechtlichen Vorgaben lassen dem deutschen Gesetzgeber nur bedingt Spielraum.[183]

Zum einen hat bereits der BGH im Jahr 2004 geurteilt, dass das Haftungsprivileg des TMG auf Unterlassungs- und Beseitigungsansprüche keine Anwendung findet. Dass die Unterlassungsansprüche gegen alle Provider bestehen, schließt das Gericht in seinem Urteil aus dem Wortlaut des § 7 Abs. 2 Satz. 2 TMG.[184] Dieser setzt die europäischen Vorgaben der E-Commerce-RL um. Demnach hat der Diensteanbieter nach allgemeinen Gesetzen auch dann Informationen zu entfernen oder deren Nutzung zu sperren, wenn ihn keine Verantwortlichkeit trifft. [185]

Zum anderen hat der EuGH bereits im Jahr 2014 die Frage beantwortet, ob Unterlassungsansprüche gegen Diensteanbieter trotz des Providerprivilegs erhoben werden können.[186] Es ist per se nicht unzulässig, Access Provider in die Pflicht zu nehmen, Rechtsverletzungen zu verhindern, womit die Entscheidung des BGH vom EuGH bestätigt wurde. Somit würde die deutsche Gesetzgebung, im Falle eines Verzichts auf Unterlassungsansprüche, gegen europarechtliche Vorschriften verstoßen. Eine Änderung der Vorschrift des § 7 Abs. 2 TMG kann damit ausgeschlossen werden.[187]

Ein weiterer Grund, warum ein völliger Verzicht auf Unterlassungsansprüche durch den nationalen Gesetzgeber nicht möglich wäre, ist, dass der EuGH in seiner WLAN-Entscheidung klarstellt, dass es den zuständigen innerstaatlichen Behörden oder Gerichten obliegt, ein angemessenes Gleichgewicht zwischen den unionsrechtlich geschützten Grundrechten sicherzustellen.[188] Auch aus der Gesetzesbegründung zu § 8 Abs. 3 TMG geht hervor, dass ein angemessenes Gleichgewicht zwischen den Grundrechten gewahrt werden muss. Eine völlige Haftungsbefreiung der WLAN-Anbieter bei Rechtsverletzungen durch Dritte wäre nicht möglich, da einerseits die Rechteinhaber damit völlig schutzlos wären und andererseits würde sich eine völlige Haftungsbefreiung zum Schutz der WLAN-Anbieter über den Schutz der Urheberrechte stellen. Ein Gleichgewicht wird insofern geschaffen, als WLAN-Anbieter zwar von der Haftung weitgehend befreit werden, ihnen jedoch Interventionspflichten zum Schutze der Rechte Dritter mit Hilfe einer gerichtlichen oder behördlichen Anordnung aufgegeben werden.

Ferner sind auch weitere europarechtliche Vorgaben (Art. 8 Abs. 3 der Urheber-RL 2001/29/EG und Art. 11 S. 3 der Durchsetzungs-RL 2004/48/EG) zum Schutz der Urheber zu beachten, über die sich der nationale Gesetzgeber nicht ohne weiteres hinwegsetzen kann. Gemäß diesen Vorschriften sollen die Urheber die Möglichkeit haben, mit gerichtlichen Anordnungen gegen die Vermittler[189] bei Rechtsverletzungen vorzugehen.[190]

Schließlich ist zu beachten, dass der BGH im Jahr 2015 entschieden hat, dass Sperrverfügungen gegen Access Provider grundsätzlich erlassen werden können.[191] Der BGH vertrat in seiner Entscheidung die Auffassung, dass die Störerhaftung eine ausreichende Grundlage darstelle, um Access Provider bei urheberrechtlichen Verletzungen auf Grundlage von Unterlassungsansprüchen unter bestimmten Voraussetzungen dazu zu verpflichten, ihr Netz zu sperren.[192]

Sicherung des WLANs und Registrierung der Nutzenden

In der Gesetzesbegründung zu § 8 Abs. 3 TMG, die sich auf die Schlussanträge des EuGH-Generalanwalts stützt, wird klargestellt, dass eine gerichtliche Anordnung dann unzulässig ist, wenn der WLAN-Anbieter dieser nur dann nachkommen kann, wenn er sein WLAN mit einem Passwort oder mit einer Verschlüsselung sichert. In dem Punkt vertrat der EuGH eine davon abweichende Auffassung. Das Gericht hält es zum einen für angemessen, das WLAN mit einem Passwort zu sichern, um ein Gleichgewicht zwischen den kollidierenden Grundrechten herzustellen. Zum anderen sei es erforderlich, um die WLAN-Nutzenden vor Begehung vor Urheberrechtsverletzungen abzuschrecken, dass sie vor der Passwortvergabe ihre Identität offenbaren müssen. Der EuGH stellt jedoch klar, dass es sich bei der Passwortsicherung nur um eine mögliche technische Modalität handelt. Weitere technische Möglichkeiten schließt das Gericht nicht aus und überlässt deren Prüfung den zuständigen nationalen Gerichten.[193]

Es liegt die Vermutung nahe, dass sich der EuGH mit dieser Feststellung um einen Ausgleich zwischen den betroffenen Grundrechten bemüht und sich für eine Kompromisslösung entschieden hat.

Das Gericht hält zwar die Sicherung des WLANs mit einem Passwort für angemessen und wirksam, dabei handelt sich jedoch nur um eine mögliche technische Variante. Im Hinblick auf einen ständigen technologischen Fortschritt ist es überaus von Vorteil, weitere technische Maßnahmen offen zu lassen und im Fall einer gerichtlichen Anordnung über die Wirksamkeit, die zuständigen Gerichte im Einzelfall entscheiden zu lassen.

Darüber hinaus ist zu konstatieren, dass der EuGH keine Sicherung des WLANs von den Anbietern von Anfang fordert. Erst nach einer festgestellten Rechtsverletzung (um eine weitere vorzubeugen) kann der WLAN-Anbieter mittels einer gerichtlichen oder behördlichen Anordnung aufgefordert werden, den Internetanschluss mit einem Passwort zu sichern.[194]

Ferner postuliert der EuGH, dass die WLAN-Nutzenden vor der Passwortvergabe identifiziert werden müssen.[195] Die Frage, welche Anforderungen an die Überprüfung der Identität zu stellen sind, beantwortet der EuGH allerdings nicht.

Die WLAN-Anbieter werden somit vor viele neue Fragen und Probleme gestellt: Wie soll die Identität in der Praxis festgestellt werden? Welche Anforderungen sind an sie zu stellen? Würde es ausreichen, nur seinen Namen vor der Passwortvergabe zu nennen oder muss die Identifikation anhand gültiger Ausweise (z. B. Personalausweis oder Reisepass) erfolgen?

Es ist an der Stelle davon auszugehen, dass für eine wirksame Identifizierung der Nutzenden die bloße Nennung des Namens in der Regel nicht ausreichen wird, da die Behauptung ohne die Kontrolle gültiger Ausweispapiere kaum zu überprüfen sei. Dies hätte im Ergebnis zur Folge, dass für eine wirksame Identitätsoffenbarung die Angabe des vollständigen Namens und weiterer personenbezogener Daten erforderlich sein wird. Und dies wird wiederum die WLAN-Anbieter vor neue – datenschutzrechtliche – Fragen stellen, auf die die EuGH-Entscheidung jedoch keine Antworten liefert. In dem Zusammenhang wird zunächst die Frage zu klären sein, auf Grundlage welchen Erlaubnistatbestandes die Verarbeitung und Speicherung personenbezogener Daten der WLAN-Nutzenden zur Identifizierung erlaubt ist.[196] Des Weiteren wird der Frage nach der Aufbewahrungsfrist nachzugehen sein: Wie lange sollen personenbezogene Daten, die vom WLAN-Anbieter für die Identifizierung erhoben wurden, aufbewahrt werden, um die Rechtverletzungen nachträglich zurückverfolgen[197] und die Identitätsnachweise gegebenenfalls dem Gericht als Beweis anbieten zu können.

Abschließend ist festzuhalten, dass die WLAN-Anbieter in Zukunft nicht nur mit datenschutzrechtlichen Fragen konfrontiert werden, sondern es bleibt für sie zunächst ungewiss, welche Auswirkungen die Entscheidung des EuGH im Hinblick auf die Passwortsicherung des WLAN-Anschlusses auf die Rechtslage in Deutschland haben wird. Die

Unzulässigkeit, dass die WLAN-Anschlüsse nicht mit einem Passwort gesichert werden dürfen, um mittels einer gerichtliche Anordnung weiterer Rechtsverstöße zu verhindern oder zu vermeiden, hat zwar keinen direkten Eingang in § 8 Abs. 3 TMG gefunden, sondern nur in die Gesetzesbegründung. Allerdings kann nicht ohne Weiteres davon ausgegangen werden, dass die nationalen Gerichte davon auch Gebrauch machen werden, denn die Gesetzesbegründung ist für sie nicht bindend und nur eingeschränkt relevant.

Abmahnungen

Im Hinblick darauf, dass sich die Störerhaftung beim Betrieb offener WLANs zu einem profitablen Geschäftsmodell der Abmahnindustrie entwickelt hat, stellt sich letztlich die

Frage, ob nach dem EuGH-Urteil jede „Hintertür" für die Abmahnindustrie nun verschlossen bleibt. Dies wird jedoch nicht der Fall sein, da für die Durchsetzung der Untersagung weiterer Rechtsverstöße gegen die WLAN-Anbieter gerichtliche oder behördliche Anordnungen mit Passwort- und Identifizierungspflicht der WLAN-Nutzenden auch weiterhin erwirkt werden können. Da der EuGH den Geschädigten die Möglichkeit einräumt, die Erstattung der anfallenden Abmahn- und Gerichtskosten vom WLAN-Anbieter zu verlangen, wird es bei der Entwicklung der Abmahnpraxis vor allem darauf ankommen, wer diese zu tragen hat.[198] Sollten die Gerichte tatsächlich so entscheiden, dass die entstandenen Kosten dem WLAN-Anbieter auferlegt werden, würde es im Ergebnis bedeuten, dass sich die Lage der (gewerblichen) Anbieter offener WLANs nach der EuGH-Entscheidung insgesamt verschlechtert hat. Dies ist darauf zurückzuführen, dass sie von nun an bei Rechtsverletzungen durch Dritte nicht nur der Gefahr von Abmahnungen und den damit verbundenen Kosten ausgesetzt sind, sondern im Falle einer gerichtlichen oder behördlichen Anordnung zudem einer Passwort- und Identifizierungspflicht nachkommen müssen.

4.3 Strafrechtlicher Rahmen

Die haftungsrechtlichen Konsequenzen standen bislang im Zentrum der öffentlichen Diskussion. Nicht im Fokus stand bislang die Strafbarkeit der Angreifer, die sich öffentliche WLANs zu Nutze machen, um die Nutzenden missbräuchlich auszuspähen, deren Daten abzufangen oder sich Zugriff auf die Nutzerendgeräte zu verschaffen. Der Abschnitt wird zeigen, dass das Strafgesetzbuch (StGB) nach derzeitiger Rechtslage nur eine unzureichende Handhabe gegenüber derartigen Angreifern gewährt.[199]

4.3.1 Ausspähen, Abfangen von Daten und deren Vorbereitung, § 202a-c StGB

Eine Person macht sich *nicht* wegen Ausspähens von Daten nach § 202a StGB strafbar, da sie sich nicht unbefugt Zugang zu einem WLAN verschafft, das gegen unberechtigten Zugang besonders gesichert ist. Zwar kann ein Passwort grundsätzlich eine solche besondere Zugangssicherung darstellen; nicht jedoch dann, wenn ein Passwort für jeden potenziellen Nutzenden ohne jegliche Hindernisse frei zugänglich ist, wie dies häufig in Hotels und Cafés üblich ist.

Das unerlaubte Abfangen von Nutzerdaten aus WLANs ist nach § 202b StGB nur dann strafbar, wenn sich Angreifer unbefugt Daten aus einer nicht-öffentlichen Datenübermittlung verschaffen. Die Datenübertragung mittels WLAN ist nur in dem Umfang nicht-öffentlich, wie die übertragenen Daten an einen bestimmten Adressatenkreis gerichtet sind, etwa durch E-Mail, Internet-Telefonie oder Sofortnachrichtendienste wie Threema oder WhatsApp.[200] MAC-Adressen und SSIDs stellen demgegenüber eine öffentliche Datenübermittlung dar, da diese Signale an einen unbestimmten Adressatenkreis gerichtet sind.[201] Strafbar machen sich demnach alle aktiven und passiven Angreifer dann, wenn sie etwa mittels eines gefälschten Zugangspunkts in einem offenen oder geschlossenen Netzwerk eine nicht-öffentliche Datenübertragung der WLAN-Nutzenden abfangen.

Zwar besteht keine Versuchsstrafbarkeit hinsichtlich der §§ 202a und 202b StGB, jedoch kann die Vorbereitung dieser Handlungen strafbar sein. Gemäß § 202c StGB müssen hierfür Passwörter und Sicherungscodes, die den Zugang zu Daten ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, bestellt, verschafft, verkauft, überlassen, verbreitet oder sonst zugänglich gemacht werden. Somit ist bereits das Verschaffen eines Passworts oder anderer Sicherungscodes oder das Programmieren oder Modifizieren von Software zum Erstellen eines gefälschten Zugangspunkts strafbar, auch ohne dass ein Angriff auf das Netzwerk erfolgt.

4.3.2 Computerbetrug, § 263a StGB

Eine Strafbarkeit wegen Computerbetrugs nach § 263a StGB setzt voraus, dass das Ergebnis eines Datenverarbeitungsvorgangs, eine unrichtige Gestaltung des Programms, eine Verwendung unrichtiger oder unvollständiger Daten, eine unbefugte Verwendung von Daten oder ein anderweitiges unbefugtes Einwirken auf den Ablauf die Datenverarbeitung beeinflusst und damit in Absicht rechtswidriger Bereicherung das Vermögen eines anderen geschädigt wird. Das Eindringen in ein WLAN mit der Absicht, Inhalts- oder Nutzungsdaten abzufangen und auszuspähen, stellt eine unbefugte Verwendung von Daten dar, da ein Angreifer seine wahre Identität verschleiert und die Daten mangels Einwilligung oder gesetzlichem Erlaubnistatbestand ohne Berechtigung des Anbieters und der Nutzenden nutzt. Das Erstellen eines gefälschten Zugangspunkts stellt zudem eine Verwendung unrichtiger Daten dar, da es sich als authentisches Netzwerk ausgibt, ohne ein solches zu sein. Es fehlt allerdings an einer Vermögensverfügung und einem Vermögensschaden, da beim Ausspähen von Daten aus WLANs allenfalls die Persönlichkeitsrechte von Nutzerinnen und Nutzern verletzt werden, die jedoch keinen unmittelbaren Vermögensschaden darstellen.[202] Selbst beim Abgreifen von Passwörtern und anderen Zugangsdaten fehlt es an einem unmittelbaren Vermögensschaden, da weitere Schritte des Täters erforderlich sind, um Betroffene oder Dritte finanziell zu schädigen. Angreifer, die Daten aus WLANs ausspähen, werden sich somit regelmäßig nicht wegen vollendetem Computerbetrug strafbar machen; ein untauglicher, aber strafbarer Versuch nach §§ 263a Abs. 2, 263 Abs. 2 StGB käme unter der Voraussetzung in Betracht, dass Angreifer dennoch vorsätzlich eine Vermögensverfügung und einen Vermögensschaden herbeiführen wollte.[203]

4.3.3 Datenveränderung, § 303a StGB

Wegen Datenveränderung nach § 303a StGB machen sich Angreifer nur dann strafbar, wenn sie rechtswidrig Daten löschen, unterdrücken, unbrauchbar machen oder verändern. Geschützt ist in § 303a StGB die Verfügungsgewalt über und das Interesse der Berechtigten an der unversehrten Verwendbarkeit von Daten.[204] Daher ist nur der Zugriff auf den Datenspeicher der Berechtigten wie Smartphones und andere internetfähige Endgeräte geschützt, nicht hingegen der Datenübermittlungsvorgang als solcher.[205] Das Einrichten eines gefälschten Zugangspunkts kann ein Verändern von Daten allenfalls dann darstellen, wenn Angreifer dabei Manipulationen an im Netzwerk vorhandenen Daten vornehmen. Möglich ist dies etwa durch das Einschleusen von Viren und Trojanern, aber nur, sofern Daten verändert oder unbrauchbar gemacht werden. Eine versuchte Datenveränderung oder -löschung ist strafbar nach § 303a Abs. 2 StGB. Das Ausspähen des Datenverkehrs der im Netzwerk eingeloggten Nutzenden, ohne dass Veränderungen an gespeicherten Daten vorgenommen werden, ist allerdings nach § 303a StGB nicht strafbar.[206]

4.3.4 Computersabotage, § 303b StGB

Computersabotage ist strafbar, sofern eine Datenverarbeitung, die für eine(n) andere(n) von wesentlicher Bedeutung ist, erheblich gestört wird, indem entweder eine strafbare Datenveränderung nach § 303a StGB begangen wird (Nr. 1), in der Absicht jemand anderem zu schaden Daten eingegeben oder übermittelt werden (Nr. 2) oder eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar gemacht, beseitigt oder verändert wird (Nr. 3). Neben der Verwirklichung des § 303a StGB[207] ist als Tathandlung vor allem das Eingeben oder Übermitteln von Daten in Absicht der Nachteilszufügung nach § 303b Abs. 1 Satz 1 Nr. 2 StGB denkbar, das heißt bei missbräuchlicher oder unbefugter Handlungsweise.[208] Beim Errichten eines gefälschten Zugangspunkts ist dies der Fall, da das Eröffnen eines gefälschten Zugangspunkts und die Verbindung mit Endgeräten eine Datenübermittlung an diese im WLAN befindlichen Endgeräte voraussetzt. Zudem ist das Abfangen von Daten aus dem WLAN eine Datenübermittlung. Die Nachteilszufügungsabsicht des Täters muss sich nicht zwingend auf einen finanziellen Nachteil beziehen, so dass bereits das Ausspähen

gutgläubiger WLAN-Nutzender und der Missbrauch eines WLANs zum Zwecke der Ausspähung als Nachteil zu werten ist.

Wesentliche Bedeutung der Datenverarbeitung

Die Datenverarbeitung muss zudem von wesentlicher Bedeutung für die Betroffenen sein. Mögliche Betroffene können sowohl WLAN-Nutzende als auch -Anbieter sein.

Für WLAN-Nutzende ist die Verwendung öffentlicher WLANs eine Datenverarbeitung von wesentlicher Bedeutung. Nicht nur ist die zunehmende Verbreitung öffentlicher WLANs gerade dem Umstand geschuldet, dass eine jederzeitige Verbindung der eigenen Endgeräte mit dem Internet für die Mehrzahl der Nutzenden von größter Bedeutung ist, um ungehindert kommunizieren zu können oder Informationen zu beschaffen. Auch führt das kontinuierliche Aussenden von Daten der Endgeräte an potenzielle Netzwerkinfrastrukturen bei einer zunehmenden Dichte öffentlicher WLANs zu einem stetigen Überwachen, Tracking und Profiling der Nutzenden – gegebenenfalls über mehrere WLANs hinweg. Das greift tief in die private Lebensgestaltung als solche ein, da ein Überwachungsgefühl der einzelnen Betroffenen – mit Auswirkungen auf die täglichen Handlungsentscheidungen der Betroffenen – entstehen kann.

Für WLAN-Anbieter ist die Datenverarbeitung nur dann von wesentlicher Bedeutung, wenn ein kommerzielles Interesse an den Nutzerdaten nachgewiesen werden kann. Voraussetzung ist, dass *Arbeitsweise, Ausstattung und Organisation* des unmittelbar betroffenen Betriebs oder Unternehmens als WLAN-Anbieter ganz oder zu einem wesentlichen Teil *vom einwandfreien Funktionieren der Datenverarbeitung abhängen.*209 *Erhebt und nutzt das Unternehmen die Daten der Nutzenden etwa zur personalisierten Werbung in einem Kaufhaus, dann hängt die Datenverarbeitung zum Zwecke der Werbung zu einem wesentlichen Teil vom einwandfreien Funktionieren dieser Funkverbindung und dieser Datenverarbeitung ab. Zumindest für Anbieter öffentlicher WLANs mit kommerziellem Interesse an den Nutzerdaten liegt damit eine wesentliche Bedeutung der Datenverarbeitung vor. Ist die Bereitstellung eines öffentlichen WLANs für den Betrieb lediglich ein Service für die Kunden, ist die Organisation des Betriebs nicht vom Funktionieren dieser Datenverarbeitung abhängig, sodass in diesem Fall keine wesentliche Bedeutung der Datenverarbeitung vorläge.*

Erhebliche Störung der Datenverarbeitung

Eine Datenverarbeitung mit wesentlicher Bedeutung für Nutzende und Anbieter eines öffentlichen WLANs muss für eine Verwirklichung der Computersabotage erheblich gestört werden. Eine erhebliche Störung liegt vor, wenn der reibungslose Ablauf der Datenverarbeitung nicht durch Störung des Datenflusses, durch Systemabstürze, durch die Verursachung inhaltlich unrichtiger Ergebnisse oder durch eine Verhinderung der Datenverarbeitung unerheblich beeinträchtigt ist[210] und sie sich nicht ohne großen Aufwand entdecken und beheben lässt.[211]

Für die ausgespähten Nutzenden liegt keine Störung vor, da aus deren Sicht der Datenfluss ungehindert funktioniert, weder Systemabstürze verursacht noch Datenverarbeitungen verhindert werden und auch keine unrichtigen Datenverarbeitungsergebnisse entstehen, solange die Nutzenden „lediglich" ausgespäht oder etwa ihr Bewegungsprofil ermittelt wird. Für die WLAN-Anbieter liegt eine Störung dann vor, wenn ihnen Daten entzogen werden, zum Beispiel, wenn Geschäftsleuten mittels gefälschter Zugangspunkte Daten der Kunden vorenthalten werden. Stellen Anbieter das WLAN hingegen aus gemeinnützigen Zwecken oder nur deshalb zur Verfügung, damit die Kundschaft im Internet surfen kann, etwa in einem Café, das offenes WLAN als Service zum Surfen im Internet anbietet, wird die Datenverarbeitung für die Anbieter nicht gestört, da für diese der Ablauf der Datenverarbeitung weiterhin reibungslos funktioniert und ihr Funknetzwerk weiterhin zur Verfügung steht. Daher ist für die Annahme der Störung entscheidend, für welche Zwecke Anbieter ihr WLAN öffnen.

Strafbarkeit bei Computersabotage

Im Ergebnis kann sich somit ein Angreifer wegen Computersabotage strafbar machen, indem unbefugt und missbräuchlich Daten in das Netzwerk von WLAN-Anbietern eingegeben oder übermittelt und Anbieter damit geschädigt werden. Dies gilt aber nur, wenn ein öffentliches WLAN angeboten wird, um die Daten der Nutzenden kommerziell zu nutzen. Eine Schädigung der Nutzenden ist somit nicht ausreichend für eine Strafbarkeit, da diese nicht erheblich gestört werden.

4.3.5 Sonstige Straftatbestände

Eine Störung von Telekommunikationsanlagen nach § 317 StGB kommt nicht in Betracht. Zwar ist ein Funknetzwerk eine solche Telekommunikationsanlage,[212] da diese öffentlichen Zwecken dient, wenn ihr Betrieb im Interesse der Allgemeinheit liegt. Jedoch ist eine Einwirkung auf die Sachsubstanz notwendig, eine unbefugte oder missbräuchliche Nutzung der Anlage fällt nicht hierunter.[213] Da ein Ausspähen der über das Netzwerk übermittelten Daten mittels Hard- oder Software keine Einwirkung auf die Sachsubstanz der Funknetzverbindung verursacht, scheidet eine Strafbarkeit nach § 317 StGB aus.

Der Angreifer macht sich auch nicht wegen Verletzung des Fernmeldegeheimnisses nach § 148 Abs. 1 Nr. 1 TKG (Telekommunikationsgesetz) strafbar. Zwar ist ein WLAN eine Funkanlage und fällt damit in den geschützten Bereich der Norm. Allerdings adressiert § 148 TKG nur die Betreiber der Funkanlage.[214] Auf Angreifer als unbefugte Nutzende ist § 148 TKG nicht anwendbar.[215] Selbst wenn der Angreifer oder die Angreifern von der Vorschrift adressiert würde, wären zwar die Kommunikationsinhalte der WLAN-Nutzenden geschützt, nicht jedoch die mit dem Einwählen in ein WLAN anfallenden Metadaten, die für gewöhnlich bei gefälschten Zugangspunkten erhoben werden und zum Profiling und Tracking der WLAN-Nutzenden missbraucht werden können.

Schließlich verbietet §§ 43 Abs. 2 Nr. 1-4, 44 Abs. 1 BDSG (Bundesdatenschutzgesetz) das unbefugte Erheben und Verarbeiten, Bereithalten, Verschaffen und das Erschleichen von Daten durch unrichtige Angaben, die nicht allgemein zugänglich sind, wenn der Täter gegen Entgelt oder in der Absicht handelt, sich oder andere zu bereichern oder andere zu schädigen. „Nicht allgemein zugänglich“ sind Daten aus WLANs dann, wenn sie gegen Zugriff geschützt sind. Setzen sich Angreifer über eine Zugangssperre hinweg, greifen sie auf nicht allgemein zugängliche Daten zu und machen sich bei Vorliegen einer Bereicherungs- oder Schädigungsabsicht strafbar. Bei offenen WLANs, die unverschlüsselt betrieben werden, ist ein Angriff auf das Netzwerk wegen der öffentlichen Zugänglichkeit der Daten hingegen straflos.

4.3.6 Nicht-erfüllte Straftatbestände

Angriffe auf offene, für alle frei zugängliche WLANs erfüllen weder die Tatbestände des Ausspähens von Daten nach § 202a StGB, das Abfangen von Daten nach § 202b StGB, den Computerbetrug nach § 263a StGB, die strafbare Datenveränderung nach § 303a StGB, die Störung von Telekommunikationsanlagen nach § 317 StGB noch den unbefugten Datenumgang nach §§ 43 Abs. 2 Nr. 1 bis 4, 44 StGB oder das Abhörverbot nach § 148 Abs. 1 Nr. 1 TKG. Die Computersabotage nach § 303b StGB erfasst demgegenüber nur offene WLANs mit kommerzieller Ausrichtung.

4.4 Datenschutzrechtlicher Rahmen

Die öffentliche Diskussion dreht sich, soweit ersichtlich, schwerpunktmäßig um die haftungsrechtlichen Fragen öffentlicher WLANs. Neben den strafrechtlichen Aspekten kommen dabei auch die datenschutzrechtlichen Fragestellungen zu kurz. Allerdings darf nicht verkannt werden, dass die haftungsrechtlichen Probleme auch Auswirkungen

auf die Belange des Datenschutzes haben, wie sich durch das Urteil des Europäischen Gerichtshofs vom 15.09.2016 gezeigt hat.

Daher wird im Folgenden dargestellt, welchen datenschutzrechtlichen Regelungen der Betreiber eines öffentlichen WLANs unterliegt. Wie Abschnitt 3.2 gezeigt hat, besteht bei einer Reihe von Akteuren ein Interesse daran, anfallende Nutzerdaten zu analysieren um Geschäftsprozesse zu optimieren, Werbemaßnahmen zu überprüfen oder Preise anzupassen. Dieses Interesse kann insbesondere dann geweckt werden, wenn öffentliche WLANs eine größere Verbreitung finden und so auch der Markt für entsprechende Analysedienste wächst. Der Betreiber des öffentlichen und eventuell kostenlosen WLANs kann sich mithilfe solcher Analysedienste dann nicht nur davon einen Mehrwert erhoffen, dass ein öffentliches WLAN ggf. zusätzliche Kundinnen und Kunden anzieht oder diese zu einer längeren Verweildauer im jeweiligen Geschäft motiviert. Er kann auch darüber hinaus für sich Mehrwerte aus der Analyse der über sein WLAN stattfindenden Kommunikation, bei der auch personenbezogene Daten anfallen, erzeugen. Dagegen stehen die Interessen der Nutzerinnen und Nutzer des öffentlichen WLANs, die befürchten müssen, dass ihr Grundrecht auf informationelle Selbstbestimmung verletzt wird, indem beispielsweise ihr Kaufverhalten analysiert wird, Bewegungsprofile ermöglicht werden und darauf aufbauend sogar ihr Verhalten beeinflusst wird. Im Ergebnis wird gezeigt, dass Betreiber eines öffentlichen WLANs dem Telekommunikationsrecht und dem Fernmeldegeheimnis unterliegen und eine Nutzung der Daten nur unter sehr engen Voraussetzungen und für bestimmte Zwecke möglich ist und für die Analyse von Kundenverhalten durch Mobile Location Analytics keine Rechtsgrundlage vorliegt.

4.4.1 Anwendbarkeit des Telekommunikationsrechts

Der Betrieb eines WLANs unterfällt dem Telekommunikationsrecht. Nach § 3 Nr. 22 TKG handelt es sich bei Telekommunikation um den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen. Eine WLAN-Kommunikation stellt ein solches Aussenden, Übermitteln und Empfangen von Signalen dar.[216] Die Betreiber von freien WLANs sind auch Diensteanbieter im telekommunikationsrechtlichen Sinne und unterliegen daher den telekommunikationsrechtlichen Normen.

Diensteanbieter ist nach § 3 Nr. 6 TKG „jeder der ganz oder teilweise geschäftsmäßig a) Telekommunikationsdienste erbringt oder b) an der Erbringung solcher Dienste mitwirkt". Insbesondere bei dem Inhaber eines Kaufhauses oder eines Restaurants, der seiner Kundschaft „nebenbei" ein WLAN zur Verfügung stellen, kann man sich fragen, ob diese geschäftsmäßig an der Erbringung von Telekommunikationsdiensten mitwirken. Für die Geschäftsmäßigkeit ist, wie § 3 Nr. 10 TKG klarstellt, keine Gewinnerzielungsabsicht erforderlich, sondern lediglich, dass ein Angebot nachhaltig für Dritte zur Verfügung gestellt wird.

Das ist dann nicht der Fall, wenn es sich lediglich um ein Angebot im Einzelfall handelt,[217] also wenn z. B. im Rahmen einer Veranstaltung einmalig für die Teilnehmenden ein WLAN-Zugang zur Verfügung gestellt wird. Geschäftsmäßigkeit liegt aber vor, wenn ein Kaufhaus, ein Restaurant, Krankenhäuser oder vergleichbare Anbieter ihren Kunden oder Patienten einen WLAN-Zugang ermöglichen wollen. Weil keine unmittelbare oder mittelbare Gewinnerzielungsabsicht erforderlich ist, kommt es nicht darauf an, ob der Diensteanbieter ein Entgelt verlangt, das WLAN mit der Motivation der Absatzsteigerung oder aus altruistischen Gründen anbietet.

Die Voraussetzung, dass das Angebot für Dritte zur Verfügung gestellt werden muss, ist problematisch, wenn ein Arbeitgeber seinen Arbeitnehmern einen WLAN-Zugang zur Verfügung stellt. Zumindest, wenn die private Nutzung des WLAN-Zugangs erlaubt wird, sind die Arbeitnehmer allerdings auch als Privatpersonen betroffen und somit „Dritte" im Sinne der Norm.[218] Der Arbeitgeber unterliegt dann gegenüber seinen Arbeitnehmern dem Telekommunikationsrecht.

4.4.2 Fernmeldegeheimnis

Alle Diensteanbieter unterliegen dem Fernmeldegeheimnis aus § 88 TKG. Hintergrund der Norm ist das verfassungsrechtliche Fernmeldegeheimnis aus Art. 10 GG, welches unmittelbar nur den Staat bindet und im § 88 TKG seine einfachrechtliche Umsetzung findet, der auch Private unterliegen. Der Gesetzgeber ist hier also seiner Pflicht zum Schutz dieses Grundrechts nachgekommen.[219] Das Grundrecht schützt vor den besonderen Risiken einer Kommunikation, bei der die Teilnehmenden auf Vermittlungsleistungen von Dritten angewiesen sind. Diese Risiken bestehen insbesondere darin, dass heimlich auf Geheimnisse von Teilnehmenden zugegriffen und diese weitergeben werden.[220] In solch einer besonders schutzbedürftigen Situation befinden sich auch die Nutzerinnen und Nutzer eines öffentlichen WLANs. Er nutzt eine fremde Kommunikationsinfrastruktur, die es dem Diensteanbieter ermöglicht, tiefgreifende Einblicke in die darüber stattfindende Kommunikation zu erlangen.[221] Im Folgenden wird gezeigt, welche telekommunikatonsrechtlichen Regelungen dieser Situation Rechnung tragen.

§ 88 Abs. 3 TKG regelt die Pflichten, die sich für Diensteanbieter daraus ergeben, dass sie dem Fernmeldegeheimnis unterliegen. Diese betreffen einerseits die Frage, inwieweit von Inhalten und Umständen der Kommunikation Kenntnis genommen werden darf und andererseits die Zweckbindung.

Diensteanbieter dürften demnach von Inhalten und den Umständen der Kommunikation nur insoweit Kenntnis nehmen, wie es für die Erbringung der Telekommunikationsdienste und deren Schutz erforderlich ist. Das Zweckbindungsgebot bedeutet, dass die Daten dann auch nur für Zwecke der Erbringung der Telekommunikationsdienste verwendet werden dürfen.

Die Vorschrift ist technikneutral gestaltet und enthält keine Angaben darüber, welche Daten für bestimmte Telekommunikationsdienste erforderlich sind. Ob dies der Fall ist, kann nur anhand einer Einzelfallbetrachtung erfolgen. Allerdings finden sich genauere Regelungen zur Erforderlichkeit personenbezogener Daten bei den §§ 91 ff. TKG.[222]

4.4.3 Schutz personenbezogener Daten

Die §§ 91 ff. TKG regeln den Schutz personenbezogener Daten für Teilnehmende und Nutzende von Telekommunikation, § 91 Abs. 1 S. 1 TKG.

Personenbezogene Daten sind in § 3 Abs. 1 BDSG definiert. Danach handelt es sich um „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person". Bei allen Daten, die bei der WLAN-Nutzung anfallen und Aussagen über das Kommunikationsverhalten des Betroffenen ermöglichen, handelt es sich um solche personenbezogenen Daten. Das gleiche gilt beispielsweise auch für IP-[223] sowie MAC-Adressen.

Wie im Bundesdatenschutzgesetz gilt auch im Telekommunikationsgesetz, dass personenbezogene Daten nur erhoben, verarbeitet, gespeichert oder genutzt werden dürfen, wenn eine Einwilligung oder eine Erlaubnisnorm vorliegt.[224]

Informationspflichten

§ 93 TKG regelt Informationspflichten der Diensteanbieter gegenüber den Teilnehmenden. Demgemäß sind Nutzerinnen und Nutzer öffentlicher WLANs bei Vertragsschluss in allgemeinverständlicher Form über Art, Umfang, Ort und Zweck der Datenerhebung zu informieren. Daneben steht es den Nutzern frei, gegenüber WLAN-Betreibenden Auskunftsansprüche nach dem Bundesdatenschutzgesetz geltend zu machen.

Unterscheidung zwischen Bestands- und Verkehrsdaten

Bei den Daten, die erhoben und verwendet werden dürfen, unterscheidet das TKG zwischen Bestands- und Verkehrsdaten. Bestandsdaten sind nach § 3 Nr. 3 TKG solche Daten, „die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung

eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden". Es handelt sich hier üblicherweise um Daten zur Leistungserbringung und Abrechnung, also z. B. Name, Vorname, Anschrift und Bankverbindung.[225]

Verkehrsdaten sind in § 3 Nr. 30 TKG legal definiert. Es handelt sich um solche Daten, „die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden". Verkehrsdaten enthalten Informationen darüber, wer mit wem kommuniziert hat.[226] Dazu gehören z. B. IP-Adressen, MAC-Adressen, Beginn und Ende einer Verbindung und übermittelte Datenmengen.

Schutz von Bestandsdaten

Die Verarbeitung von Bestandsdaten ist in § 95 TKG geregelt. Sie unterliegen selbst nicht dem Fernmeldegeheimnis, dürfen aber ebenfalls nur erhoben werden, wenn es erforderlich ist, um einen Vertrag über Telekommunikationsdienste zu begründen, inhaltlich auszugestalten, zu ändern oder zu beenden. Wird ein WLAN-Zugang kostenpflichtig angeboten, dürfen die für die Abrechnung erforderlichen Daten erhoben werden.

Hier wirken sich dann auch die haftungsrechtlichen Fragen aus. Wie oben ausgeführt (Abschnitt 4.2.2), hat der EuGH in seinem Urteil zur WLAN-Haftung eine Anordnung gegenüber einem WLAN-Betreiber für rechtmäßig erachtet, mit der ihm aufgegeben wird, zur Verhinderung von Urheberrechtsverstößen sein Netzwerk mit einem Passwort zu schützen und dieses Passwort erst nach der Offenbarung der Identität der Nutzenden herauszugeben.[227] Fraglich ist aber, wie diese Identitätsfeststellung in der Praxis vorgenommen werden kann. Der EuGH schweigt hierzu und gibt als Prüfungsmaßstab lediglich vor, dass die Maßnahme die Nutzenden davon abschrecken soll, Urheberrechte zu verletzen. Wie oben richtig festgestellt wurde, wirft dies für die Praxis eine Vielzahl von Fragen auf, die die Rechtsunsicherheit für WLAN-Anbieter noch verschlimmern dürften.

Es ist zunächst kritisch anzumerken, dass der EuGH in seiner Abwägung auf der einen Seite das Grundrecht auf Schutz des geistigen Eigentums nach Art. 17 Abs. 2 der Charta der Grundrechte der Europäischen Union anführt und auf der anderen Seite das Recht auf unternehmerische Freiheit nach Art. 16 des WLAN-Betreibers und die Informationsfreiheit nach Art. 11 der Nutzenden anführt. Das Grundrecht auf Datenschutz nach Art. 8 der Charta wird mit keinem Wort erwähnt, obwohl die vom EuGH für rechtmäßig erachtete Maßnahme darin besteht, die Identität der WLAN-Nutzenden durch die WLAN-Betreibenden erheben zu lassen. Eine Prüfung des Datenschutzgrundrechts hätte sich damit geradezu aufgedrängt. Der Fall berührt somit keineswegs bloß die Informationsfreiheit aus Art. 11 der Charta.

Mit der genannten Abschreckungsfunktion der Nutzeridentifikation, auf die der EuGH seine Entscheidung stützt, ließe sich z. B. argumentieren, dass diese nur dann ihre Wirkung entfalten könne, wenn vor der Herausgabe des WLAN-Passwortes an die Nutzenden durch Vorlage des Personalausweises Nachname, Vorname und Wohnort nachgewiesen werden. Ferner könnte man argumentieren, dass auch eine Verknüpfung zu den benutzten Geräten hergestellt werden müsse, damit die Nutzerin oder der Nutzer bei einer durch ihn oder sie begangenen Urheberrechtsverletzung tatsächlich identifiziert werden kann. Dann stellt sich allerdings auch die Frage, wie lange die Daten aufzubewahren sind. Die Verjährungsfrist für Unterlassungsansprüche nach dem Urhebergesetz beträgt regelmäßig drei Jahre.[228] Damit unterlägen die Nutzerinnen und Nutzer öffentlicher WLANs faktisch einer Vorratsdatenspeicherung. Andererseits hat der EuGH seine Lösung nicht mit der Durchsetzung von Unterlassungsansprüchen begründet, sondern lediglich mit der Abschreckungswirkung einer Identifizierung. Dafür könnten auch kürzere Aufbewahrungsfristen ausreichend sein. Man könnte allerdings auch argumentieren, dass die Daten sofort gelöscht werden könnten, solange die Nutzenden dies nicht wissen. Denn auch dann könnte die Identifikation ihre Abschreckungswir-

kung entfalten. Diese Überlegungen machen es umso unverständlicher, dass der EuGH das Recht auf Datenschutz in seine Abwägung nicht hat einfließen lassen.

Fraglich ist auch, welche Rechtsgrundlage für die Erhebung dieser Daten überhaupt einschlägig sein soll. Die Identifikation wäre nämlich eigentlich nicht erforderlich zur Begründung, inhaltlichen Ausgestaltung oder Beendigung eines Vertragsverhältnisses im Sinne des § 95 Abs. 1 TKG. Allerdings hat der EuGH zu den Datenschutzregelungen im TMG entschieden, dass die dortigen Zweckbegrenzungen zu eng sind, weil sie keine Abwägung der berechtigten Interessen der verantwortlichen Stelle mit den Interessen der Betroffenen erlauben.[229] Deshalb ist fraglich, ob die strikten Regelungen des TKG vor dem EuGH Bestand hätten. Weiterhin kann nach § 95 Abs. 4 TKG die Vorlage eines Ausweises bei der Begründung eines Vertragsverhältnisses durch den Diensteanbieter verlangt werden und es darf eine Kopie des Ausweises erstellt werden. Voraussetzung hierfür ist aber, dass dies zur Überprüfung der Angaben des Teilnehmers bzw. der Teilnehmerin erforderlich ist. Hintergrund der Regelung ist, dass Telekommunikationsdiensteanbieter üblicherweise in Vorleistung gehen und deshalb die Identität ihrer Kundinnen und Kunden überprüfen können müssen um Forderungsausfälle zu minimieren.[230] Mit dieser Norm kann die Vorlage des Ausweises also insbesondere bei kostenfreien WLAN-Angeboten nicht gerechtfertigt werden, weil kein Risiko eines Forderungsausfalls besteht. Bei kostenpflichtigen WLAN-Angeboten wird der Nutzer bzw. die Nutzerin des WLANs regelmäßig in Vorleistung gehen müssen, was wiederum das Risiko eines Forderungsausfalls ausschließt. Nur wenn der Anbieter eines kostenpflichtigen WLANs in Vorleistung geht, besteht tatsächlich das Risiko eines Forderungsausfalls.

Damit kann im Ergebnis nur festgestellt werden, dass das fragliche Urteil des EuGH auch aus datenschutzrechtlicher Perspektive eine Vielzahl von Fragen aufwirft und die Rechtsunsicherheit verstärkt.

Schutz von Verkehrsdaten

Verkehrsdaten dürften für die ökonomische Verwertung besonders interessant sein, sind aber sehr sensibel, weil sie Aufschluss über Inhalt und Umstände der Kommunikation geben. Die Verkehrsdaten, die erhoben werden dürfen, sind in § 96 Abs. 1 TKG abschließend aufgezählt. Darunter sind die Anschlusskennung, personenbezogene Berechtigungskennungen, Beginn und Ende der Verbindung, Datenmengen, wenn das Entgelt davon abhängt sowie die zum Aufbau und zur Aufrechterhaltung der Telekommunikation und Entgeltabrechnung notwendigen Verkehrsdaten. Sie dürfen grundsätzlich auch nur für diese Zwecke verwendet werden und müssen, wenn eine weitere Verwendung nicht erforderlich ist, nach der Beendigung der Verbindung unverzüglich gelöscht werden. Abs. 2 stellt klar, dass jede darüberhinausgehende Erhebung und Verwendung von Verkehrsdaten unzulässig ist.

Selbst mit einer wirksamen Einwilligung des Betroffenen ist die Auswertung von Verkehrsdaten nur zu bestimmten Zwecken zulässig, zu denen eine Analyse des Surfverhaltens nicht zählt, § 96 Abs. 3 TKG. Insbesondere das Anlegen von Kommunikationsprofilen ist grundsätzlich unzulässig.[231]

Zweckbindung

Die sich aus dem Fernmeldegeheimnis ergebende Zweckbindung gebietet, dass die Daten nur für die Erbringung von Telekommunikationsdiensten und deren Schutz verwendet werden dürfen. Von dieser Zweckbindung darf nur abgewichen werden, wenn eine gesetzliche Vorschrift eine Abweichung rechtfertigt und diese sich ausdrücklich auf Telekommunikationsvorgänge bezieht, § 88 Abs. 3 S. 2 TKG. Solche Normen finden sich insbesondere im Bereich der Geheimdienste, der Strafverfolgung und der Gefahrenabwehr.[232] Eine Rechtsgrundlage zur Verwendung der Daten beispielsweise für Zwecke der Kundenanalyse existiert aber nicht. Eine solche Kundenanalyse kann daher nur erfolgen, wenn die Daten vorher hinreichend anonymisiert wurden.

Allerdings lässt sich der Diensteanbieter damit auf ein nicht unerhebliches Risiko ein. Sollte sich herausstellen, dass die Anonymisierung nicht hinreichend war, kann eine Ordnungswidrigkeit vorliegen, die mit einer Geldbuße von bis zu 300.000 Euro geahndet werden kann. Darüber hinaus kann eine Strafbarkeit nach §§ 44 Abs. 1, 43 BDSG vorliegen, wenn personenbezogene Daten natürlicher Personen verarbeitet wurden. Bei der Weitergabe der Daten an Dritte kommt eine Strafbarkeit nach § 206 StGB (Verletzung des Post- oder Fernmeldegeheimnisses) in Betracht. Außerdem sieht sich der Diensteanbieter gegebenenfalls zivilrechtlichen Schadensersatz- und Unterlassungsansprüchen von Betroffenen ausgesetzt.[233]

4.4.4 Meldepflichten

Gemäß § 6 Abs. 1 TKG ist der gewerbliche Betrieb eines öffentlichen Telekommunikationsnetzes oder eines öffentlich zugänglichen Telekommunikationsdienstes anzeigepflichtig. Die Bundesnetzagentur hat sich dahingehend geäußert, eine Meldepflicht liege nicht vor, wenn an der Erbringung von Telekommunikationsdiensten lediglich mitgewirkt wird. Dies solle immer dann der Fall sein, wenn das WLAN durch den Kunden nur kurzzeitig oder vorübergehend in Anspruch genommen wird. Als Beispiele werden WLANs in Restaurants, Cafés und Hotels genannt. Werde jedoch ein Dorf über ein WLAN mit Internet versorgt oder ein stadtumfassendes WLAN betrieben, liege eine Meldepflicht vor.[234]

4.4.5 Technische Schutzmaßnahmen

Jeder Diensteanbieter muss nach § 109 TKG technische Vorkehrungen und Maßnahmen unter Berücksichtigung des Standes der Technik treffen um das Fernmeldegeheimnis und die personenbezogenen Daten zu schützen.

4.4.6 Vorratsdatenspeicherung

Die Regelungen zur Vorratsdatenspeicherung von Verkehrsdaten dürften auf die Betreiber von öffentlichen WLANs regelmäßig nicht anwendbar sein. Dies sieht zumindest die Gesetzesbegründung vor, die Bezug nimmt auf die oben genannte Äußerung der Bundesnetzagentur. Die Gesetzesbegründung macht sich die Ansicht der Bundesnetzagentur zu eigen, wonach der Betrieb eines WLANs in Restaurants, Cafés und Hotels kein „Erbringen" von Telekommunikationsdienstleistungen darstellt, sondern lediglich ein daran „Mitwirken".[235] Ersteres ist aber für die Pflicht zur Vorratsdatenspeicherung erforderlich.

4.4.7 Mobile Location Analytics und allgemeines Datenschutzrecht

Anders sind Fälle der sog. *Mobile Location Analytics* (Vgl. Abschnitt 3.2) zu behandeln, bei denen Anhand von Bluetooth- und WLAN-Signalen sowie sonstigen Sensoren Kundenverhalten analysiert wird.[236]

Soweit kein WLAN-Zugang zur Verfügung gestellt wird, liegt auch kein Telekommunikationsdienst vor, weswegen die allgemeinen Vorschriften des BDSG anwendbar sind. Auch hier gilt, dass personenbezogene Daten nicht ohne Erlaubnisnorm oder Einwilligung erhoben, verarbeitet oder genutzt werden dürfen. Nachfolgend wird gezeigt, wer für den Betrieb derartiger Mobile Location Analytics verantwortlich ist und untersucht, welche datenschutzrechtlichen Rechtsgrundlagen zur Rechtfertigung dieser Datenverarbeitungen in Betracht kommen.

Verantwortlichkeit

Grundsätzlich ist der jeweilige Ladeninhaber für die Datenverarbeitung verantwortlich. Das gilt auch dann, wenn er ein anderes Unternehmen mit der Erhebung der Daten und der Analyse beauftragt. Nach § 3 Abs. 7 BDSG ist die Person oder sonstige Stelle verantwortlich, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder

nutzt oder dies durch andere im Auftrag vornehmen lässt. Die Entscheidung darüber, ob, in welchem Umfang und mit welchen Sensoren Daten zur Kundenanalyse in seinem Geschäft erhoben werden, liegt bei ihm. Er kann auch darüber bestimmen, ob er dies selbst durchführen möchte, oder dies durch andere vornehmen lässt.

Rechtsgrundlagen nach dem Bundesdatenschutzgesetz

Eine spezielle Rechtsgrundlage für diese Art der Datenerhebung existiert nicht, weshalb die allgemeinen Erlaubnistatbestände des § 28 BDSG zu prüfen sind.

Nach § 28 Abs. 1 S. 1 Nr. 1 BDSG ist das Verarbeiten personenbezogener Daten zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Begibt sich ein Kunde oder eine Kundin in ein Geschäft, in dem die o. g. Analysen vorgenommen werden, kann dadurch ein rechtsgeschäftsähnliches Schuldverhältnis durch Vertragsanbahnung entstehen.[237] Ein rechtsgeschäftliches Schuldverhältnis entsteht grundsätzlich erst bei Abschluss eines Vertrags, § 311 Abs. 1 BGB. In beiden Konstellationen, also z. B. wenn ein Kunde ein Geschäft betritt und beim Kauf eines Produkts, ist es grundsätzlich nicht erforderlich, dass Kundenverhalten analysiert wird. Erforderlich wäre eine solche Analyse nur dann, wenn der Verzicht auf sie unzumutbar oder nicht sinnvoll wäre.[238] Dies ist nicht der Fall, weil z. B. Kaufverträge in Kaufhäusern problemlos auch ohne die genannten Analysetechniken abgeschlossen werden können. Es wird beim Betreten eines Kaufhauses oder eines Cafés auch kein sog. *konkludenter Vertrag* geschlossen hat, der zum Inhalt hat, dass der Inhaber das Verhalten seiner Kundschaft mittels Sensoren und Big Data analysieren darf. Somit kann diese Rechtsgrundlage die Datenverarbeitung im Rahmen von Mobile Location Analytics nicht rechtfertigen.

Auf die Abwägungsnorm des § 28 Abs. 1 S. 1 Nr. 2 BDSG kann sich der Diensteanbieter grundsätzlich nicht stützen. Er könnte dies nur, wenn die schutzwürdigen Interessen der Betroffenen nicht sein Interesse an der Erhebung der Daten überwiegen. Wegen der hohen Sensibilität der erhobenen Daten werden aber regelmäßig die Interessen der Betroffenen überwiegen. Bei der angesprochenen Kundenanalyse geht es grade darum, möglichst genaue Kundenprofile zu gewinnen, um so Kundenverhalten und Kaufentscheidungen beeinflussen zu können. Zudem besteht die Gefahr einer umfassenden Überwachung der Innenstädte durch entsprechende Analysesysteme, insbesondere wenn dies durch zentrale Dienstleister geschieht, die für mehrere Ladeninhaber in einer Innenstadt tätig werden und somit nicht nur die Bewegung innerhalb eines Geschäfts verfolgen können, sondern auch die Bewegung eines Betroffenen durch die Innenstadt. Beide Punkte sprechen dafür, von einem Überwiegen der Betroffeneninteressen auszugehen. Darüber hinaus ist auch fraglich, ob solche Datenverarbeitungen überhaupt erforderlich sind, weil auch herkömmliche Methoden, wie z. B. die Befragung der Kundschaft, zur Optimierung der Geschäftsprozesse in Betracht kommen.

Nach § 28 Abs. 1 S. 1 Nr. 3 ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten zulässig, wenn es sich um allgemein zugängliche Daten handelt und das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung nicht höher wiegt als das berechtigte Interesse der verantwortlichen Stelle. Hinsichtlich der Interessenabwägung kann hier zunächst festgehalten werden, dass auch hier die eben genannten Gesichtspunkte zum Tragen kommen, mit denen ein Überwiegen der Betroffeneninteressen zu bejahen ist. Darüber hinaus ist fraglich, ob es sich um allgemein zugängliche Daten im datenschutzrechtlichen Sinne handelt. Die Norm soll die Informationsfreiheit aus Art. 5 Abs. 1 S. 1 GG schützen.[239] Allgemein zugänglich sind alle Quellen, die dazu geeignet und bestimmt sind, einem individuell nicht bestimmbaren Personenkreis Informationen zu verschaffen.[240] Als Beispiele werden in der Literatur Zeitungen, Radiosendungen, Fernsehsendungen, Telefonbücher und auch öffentlich zugängliche Internetseiten genannt.[241] Fraglich ist bereits, ob WLAN-Probe Requests dazu bestimmt sind, einem nicht bestimmbaren Personenkreis

Informationen zu verschaffen. Nutzende eines Smartphones dürften sich eher selten darüber bewusst sein, dass ihr Smartphone derartige WLAN-Signale aussendet. Wo dieses Bewusstsein fehlt, kann aber auch kein Wille für eine entsprechende allgemeine Zugänglichmachung vorliegen. Darüber hinaus dürfte auch kein unbestimmbarer Personenkreis vorliegen. Da die Probe Requests (vgl. Abschnitt 2.2.2) nur eine begrenzte Reichweite haben und man daher den Kreis der möglichen Empfänger zwar nicht als bestimmt, aber zumindest als bestimmbar betrachten könnte. Veröffentlichungen im Internet und Fernsehsendungen verfügen dagegen tatsächlich über einen unbestimmbaren Empfängerkreis.

Darüber hinaus dürfen keine rechtlichen Zugangsbeschränkungen für den Zugriff auf die Daten vorliegen.[242] Probe Requests dienen aber dem Kommunikationsaufbau, was auch für den Empfänger ohne weiteres ersichtlich ist. Sie erhalten also schon durch ihre technische Funktion eine Zweckbestimmung, die überdehnt wird, wenn die Daten zur Kundenanalyse erhoben werden.

Wird die Datenerhebung auf eine Einwilligung gestützt, muss diese vor der Erhebung der personenbezogenen Daten erfolgen[243]. Da die obengenannten Sensoren aber Daten über jeden erfassen, der in ihren Einflussbereich gerät, dürfte es praktisch nicht durchführbar sein, von jedem potentiellen Betroffenen vorher eine Einwilligung einzuholen. Konkludente Einwilligungen sind im Datenschutzrecht nicht möglich.[244] Und auch das Betreten eines Geschäfts stellt keine konkludente Einwilligung in eine solche Datenerhebung dar.

Insgesamt ist daher festzustellen, dass keine taugliche Rechtsgrundlage für die Durchsetzung von Mobile Location Analytics vorliegt.

Datenschutz-Grundverordnung

Ab dem 25. Mai 2018 gilt die neue EU-Datenschutz-Grundverordnung (DSGVO), Art. 99 Abs. 1 DSGVO. An dieser Stelle soll nur schlaglichtartig auf einige Regelungen eingegangen werden, die in den hier beleuchteten Fällen eine Rolle spielen können. Zunächst ist festzustellen, dass die DSGVO sich nicht auf die Anwendbarkeit der Datenschutzvorschriften TKG auswirkt, Art. 95 DSGVO. So lange also nach dem oben genannten für die Bereitstellung eines WLAN-Zugangs das TKG anwendbar ist, wird sich dies durch die DSGVO nicht ändern. Die Änderungen können sich daher nur auf die Fälle von Mobile Location Analytics auswirken.

Hinsichtlich der Rechtsgrundlagen ist zunächst festzustellen, dass sich keine Rechtsgrundlage mehr findet, die auf die allgemeine Zugänglichkeit von Daten als Tatbestandsvoraussetzung abstellt. Art. 6 Abs. 1 f) DSGVO regelt allerdings wieder eine erlaubte Verarbeitung aufgrund einer Interessenabwägung. Während § 28 Abs. 1 S. 1 Nr. 3 BDSG das Überwiegen der Betroffeneninteressen nur anerkennt, wenn dies „offensichtlich“ ist, wird in Art. 6 Abs. 1 f) DSGVO neutral formuliert, dass die Interessen der Betroffenen nicht überwiegen dürfen. Für § 28 Abs. 1 S. 1 Nr. 3 BDSG wird vertreten, dass die verantwortliche Stelle nicht zu einer intensiven Einzelfallprüfung verpflichtet ist, sondern lediglich eine summarische Prüfung vornehmen muss[245] Für Art. 6 Abs. 1 f) DSGVO wird sich diese Ansicht nicht aufrechterhalten lassen, da diese Norm keine der genannten Einschränkungen enthält. Es ist eine vollumfängliche Interessenabwägung vorzunehmen. Im Rahmen der Abwägung wäre daher weiterhin von einem Überwiegen der Betroffeneninteressen auszugehen. Hinsichtlich der Einwilligung legt Art. 7 DSGVO Bedingungen für deren Wirksamkeit fest, die die Hürden für die Wirksamkeit noch vergrößern. Daneben bleiben die obengenannten Probleme der Einholung einer wirksamen Einwilligung bestehen. Nach Abs. 1 obliegt dem Verantwortlichen die Beweislast für das Vorliegen der Einwilligung. Abs. 2 schreibt vor, dass das Ersuchen um die Einwilligung in verständlicher Form und in einer klaren und einfachen Sprache erfolgen muss und Abs. 4 legt fest, dass für die Beurteilung der Freiwilligkeit zu prüfen ist, ob die Erfüllung eines Vertrages von einer Einwilligung zu einer nicht erforderlichen Datenverarbeitung abhängig ist. Dadurch soll verhindert werden, dass

Nutzende mit ihren Daten zahlen.[246] Wer einen Dienst nutzen möchte, soll dafür keine Einwilligung erteilen müssen, die eine nicht erforderliche Datenverarbeitung legitimieren soll. Darüber hinaus sind keine weiteren Rechtsgrundlagen in der DSGVO ersichtlich, die Mobile Location Analytics rechtfertigen könnten.

Entwurf der e-Privacy-Verordnung

Der aktuelle Entwurf der E-Privacy-Verordnung[247] sieht nach Art. 2 vor, dass die Verordnung auf die Verarbeitung aller Inhalts- und Metadaten Anwendung findet, die bei der Benutzung elektronischer Kommunikationsdienste entstehen und erfasst damit auch die Kommunikation über WLAN. Sie soll gleichzeitig mit der DSGVO Geltung erlangen.

Der Entwurf sieht eine Regelung für Mobile Location Analytics vor. Nach Art. 8 Abs. 2 der Verordnung ist die Erhebung von Informationen, die Endgeräte zum Aufbau einer Verbindung aussenden zwar grundsätzlich verboten. Es gibt aber zwei Ausnahmen. Die erste und sehr sinnvolle Ausnahme ist dann gegeben, wenn die Erhebung der Informationen zum Aufbau einer Verbindung erforderlich ist. Die zweite Ausnahme betrifft Mobile Location Analytics. Dies soll zulässig sein, wenn es einen hervorgehobenen und deutlichen Hinweis gibt, der die Modalitäten der Erhebung, ihre Zwecke, den Verantwortlichen und alle weiteren Informationen nach Art. 13 DSGVO enthält. Zudem soll darüber informiert werden, was die betroffenen Personen tun können, um die Erhebung zu beenden oder zu beschränken.

Die Regelung ist nicht gelungen, weil sie zur Legitimation einer Datenverarbeitung lediglich Transparenz fordert und selbst diese Transparenz kann nicht effektiv hergestellt werden. So werden z. B. die wenigstens Besucher eines Einkaufszentrums einen am Eingang befindlichen Hinweis überhaupt wahrnehmen. Von den Besuchern, die ihn wahrnehmen werden wiederum die wenigsten sich die Mühe machen wollen, diesen zu verstehen. Doch selbst wenn betroffene Personen den Hinweis wahrnehmen und ihn verstehen verbleibt ihnen letztlich nur die Wahl, eine Überwachung in Kauf zu nehmen, einen überwachten Bereich nicht zu betreten oder ihre Geräte zu deaktivieren. Je höher der Verbreitungsgrad dieser Form der Überwachung wird, desto schwieriger wird es für die betroffenen Personen, auf Alternativen auszuweichen. Zumindest bei einem hohen Verbreitungsgrad kann also von Selbstbestimmung durch die betroffenen Personen keine Rede mehr sein.

Etwas anderes ergibt sich auch nicht daraus, dass betroffene Personen über Selbstschutzmaßnahmen informiert werden sollen. Der Wortlaut sieht nämlich nicht vor, dass Möglichkeiten zur Beendigung oder Beschränkung der Erhebung geschaffen werden müssen. Gibt es die Möglichkeiten nicht, kann lediglich darüber informiert werden, dass Kunden ihre Smartphones ausstellen können, weshalb sich durch diese Regelung kaum Konsequenzen für den Verantwortlichen ergeben.

5 Mögliche technische Gegenmaßnahmen

Zum Zwecke des Schutzes des digitalen Datenverkehrs vor unbefugter Beobachtung, Tracking und gezielter Manipulation sind seit der ursprünglichen Version der WLAN 802.11-Norm aus dem Jahr 1997 zahlreiche technische Gegenmaßnahmen vorgeschlagen und z. T. auch umgesetzt worden. Dieser Abschnitt fasst Beispiele derartiger Techniken zusammen, die dabei helfen können, in öffentlichen WLANs sicherer unterwegs zu sein. Dabei werden zunächst mögliche (Selbst-)Datenschutzpraktiken sowie Datenschutzeinstellungen am WLAN-Router vorgestellt (Abschnitt 5.1). Es werden zudem existierende Sicherheitsprotokolle für Funknetzwerke nach den IEEE 802.11-Standards (Abschnitt 5.1.3) sowie Schutzmöglichkeiten aus dem Bereich Web-basierter Systeme beleuchtet (Abschnitt 5.3). Abschließend werden auf Vorschläge bzw. Forschungsarbeiten eingegangen, die sich speziell mit Schutz- bzw. Erkennungsmöglichkeiten vor bzw. von Evil Twin-Angriffen beschäftigen (Abschnitt 5.4).

5.1 Mögliche (Selbst-)Datenschutz-Praktiken am Nutzergerät und Datenschutzeinstellungen am WLAN-Router

5.1.1 Ausschalten des WLAN-Adapters am Nutzerendgerät

Die sicherste Möglichkeit, sich vor Angriffen in öffentlichen WLANs zu schützen ist es, den WLAN-Adapter am eigenen Endgerät auszuschalten.[248] Dadurch kann das Endgerät keine Probe Request-Nachrichten mehr aussenden oder Beacon-Nachrichten vom AP empfangen, wodurch Angriffe verhindert werden. Nutzende verlieren damit allerdings auch den Komfort und weitere Möglichkeiten, die öffentliche WLANs mit sich bringen.

Da auf Nutzerseite ein großes und insbesondere angesichts wachsender Datenmengen auch äußerst legitimes Interesse daran besteht, öffentliches WLAN zu nutzen, kann das Abschalten des WLAN-Adapters nicht als eine akzeptable Schutzmöglichkeit in Frage kommen.

5.1.2 Hidden SSID – Verbergen der Netzwerknamen

Hidden SSID (auf Deutsch: Versteckter WLAN-Name) ist eine Maßnahme der Kategorie Sicherheit mittels Verschleierung (Security by Obscurity) und dient dazu, das Aussenden bzw. die Bekanntgabe der SSID eines WLANs zu verhindern. Der AP sendet dabei keine Beacon-Nachrichten mit SSID und weiteren Identifikationsdaten mehr aus. Hinter der Hidden SSID-Methode steckt die Idee, den WLAN-Namen vor illegitimen Entitäten (also z. B. vor möglichen Angreifern) geheim zu halten und diese somit davon ab zu halten, Evil Twin-APs aufzubauen und zu betreiben.

Allerdings stellt Hidden SSID keine effektive Option für die sichere Nutzung öffentlicher WLANs dar. Denn erstens ist Hidden SSID per se mit Komfortverlust assoziiert, da WLAN-Nutzende die SSID manuell bei der Konfiguration ihre Endgeräte korrekt eintragen müssen, was umso unpraktischer ist, je länger und/oder komplizierter ein WLAN-Name ist. Zweitens ist die Hidden SSID-Methode als Schutzmaßnahme nur bedingt effektiv, da sowohl aktive als auch passive Angreifer ohne große Mühe die SSID ermitteln können, indem Sie die Kommunikation zwischen anderen WLAN-Clients und dem betreffenden WLAN-AP bei der die SSID übermittelt wird, abgreifen und protokollieren. Alternativ könnten Angreifer aber auch bestehende Verbindungen von WLAN-Nutzenden stören und somit eine erneute Anmeldung mit dem AP erzwingen, wobei die SSID übermittelt wird, die wiederum vom Angreifer abgefangen werden kann. Auf-

grund dieser Schwachstellen gilt auch die Hidden SSID-Methode aus Sicht der IT-Security als keine zuverlässige Sicherheitsvorkehrung.

5.1.3 Reichweite des WLAN-Signals beschränken

Eine weitere Option, um IT-Sicherheitsbedrohungen gegen WLAN-Infrastrukturen und Dienste zu minimieren, ist, die Reichweite des WLAN-Signals auf das notwendigste geographische Gebiet (Gebäude, Einkaufszentrum usw.) zu beschränken. Je kleiner der WLAN-Funkbereich desto geringer ist die Wahrscheinlichkeit, dass unautorisierte Akteure die WLAN-Infrastruktur orten und in den Funkbereich eindringen. Hilfreich ist diese Schutzoption insbesondere in Szenarien in denen Angreifer willkürlich und großflächig nach WLAN-Hotspots suchen. Allerdings ist sie wirkungslos gegen Angreifer, die Zugriff auf den WLAN-AP haben und daher bereits mit dem AP interagieren.

5.1.4 MAC-Adressen-Hashing und MAC-Adressen-Randomisierung

MAC-Adressen sind weltweit eindeutige Kennungen für die jeweiligen Netzwerkkarten bzw. (vernetzte) Geräte aller Art. MAC-Adressen sind prinzipiell permanent und lassen sich daher sehr gut einsetzen um WLAN-fähige Endgeräte wieder zu erkennen und zu verfolgen. So stellt die Erfassung und Verknüpfung von MAC-Adressen die Grundlage neuartiger standortbasierter Dienste, mit der Möglichkeit, Rückschlüsse über On- und Offline-Aktivitäten der WLAN-Nutzenden zu ziehen (siehe Abschnitt 3) dar. Um dem entgegenzuwirken, sind zwei hash-basierte Pseudonymisierungsansätze zum Identitätsschutz in WLANs vorgeschlagen worden – Die MAC-Adressen-Randomisierung (kurz: MAC-Randomisierung) und das Hashing von MAC-Adressen, wobei MAC-Adressen-Randomisierung als proaktiver und Hashing als a posteriori Schutz betrachtet werden. Während die MAC-Adressen-Randomisierung typischerweise als Funktionalität im Betriebssystem integriert ist und somit durch die Nutzenden unmittelbar verwendet werden kann, wird das Hashing von MAC-Adressen dagegen durch die WLAN-Betreibenden vorgenommen.

MAC-Adressen-Hashing

Durch das Hashing (deutsch: kryptografisch „zerhacken“) von MAC-Adressen erhoffen sich WLAN-Betreibende zum einen, dem beachtlichen Sicherheitsrisiko der Speicherung von MAC-Adressen in unverschlüsselter Form entgegenzuwirken und zum anderen, die von ihnen gesammelten MAC-Adressen auf eine Weise zu speichern, dass selbst bei einem Angriff auf Ihre Datenbanken sensitive Kundendaten nicht offengelegt werden können. Zu diesem Zweck kommen häufig kryptographische Hashverfahren zum Einsatz.

Die Herausforderungen dabei sind allerdings vergleichbar mit jenen Herausforderungen, die sich bei einer hash-basierten Speicherung von Passwörtern ergeben: Als Hashfunktion wird i. d. R. eine sichere kryptographische Hashfunktion eingesetzt.[249] Deren Implementierung ist in der Praxis allerdings häufig fehlerhaft, was dazu führt, dass derartige Schwachstellen mittels sog. Wörterbuchangriffe ausgenutzt werden können, wie Vorfälle auf passwortbasierte Systeme immer wieder bestätigen. Daher gilt das MAC-Adressen-Hashing, anders als von Vertretern aus der Industrie behauptet,[250] nur bedingt als wirkungsvolle Datenschutzmaßnahme.

MAC-Adressen-Randomisierung

Um die Identifizierung und Verfolgung von Geräten und Nutzenden mittels MAC-Adressen zu verhindern oder zumindest zu erschweren erlauben populäre Betriebssysteme wie iOS, Windows 10 und Android in bestimmten Fällen die Randomisierung der MAC-Adresse. Beispielsweise kann die Verwendung von verschiedenen zufällig generierten MAC-Adressen für aufeinander folgende WLAN-Suchvorgänge oder für die Verbindung mit verschiedenen örtlich getrennten WLANs

die Wiedererkennung eines einzelnen Gerätes über verschiedene Suchvorgänge oder WLANs hinweg erschweren oder gar verhindern.

MAC-Randomisierung in iOS

Vorreiter bei der Randomisierung von MAC-Adressen war Apple mit der Veröffentlichung von iOS 8 im Jahr 2014. Die Randomisierung wurde dabei allerdings nur bei den Probe Requests von WLAN-Scanvorgängen vorgenommen. Von der Firma Zebra Technologies durchgeführte Tests[251] haben gezeigt, dass die Randomisierung zudem nur unter bestimmten und eher untypischen Bedingungen stattfand. So wurde die MAC-Adresse lediglich dann randomisiert, wenn das Gerät mit keinem WLAN verbunden und gerade aus dem seltenen Schlafmodus aufgewacht war. Wie in zwei Blogposts[252] beschrieben, mussten außerdem sowohl die Standort-Dienste als auch die Mobilfunk-Datenverbindung abgeschaltet sein. Ab iOS 9 findet die Randomisierung nun darüber hinaus in weiteren Fällen statt, so z. B. auch bei der Standortbestimmung und der Suche nach gespeicherten WLANs[253] auch generell dann, wenn das Gerät aktiv ist.[254] Allerdings ist die MAC-Randomisierung immer noch begrenzt auf WLAN-Suchvorgänge, weshalb eine Verfolgung von Geräten über verschiedene Netze weiterhin möglich ist.

MAC-Randomisierung in Windows 10

Seit der Veröffentlichung von Windows 10 im Juli 2015 ermöglicht nun auch Microsoft eine Randomisierung von MAC-Adressen. Unterstützt die Netzwerkkarte und der entsprechende Treiber die MAC-Randomisierung, so kann die Randomisierung in den Einstellungen global aktiviert werden, was dazu führt, dass zur Suche von WLANs zufällige MAC-Adressen genutzt werden. Darüber hinaus kann das System so konfiguriert werden, dass die MAC-Adresse für WLAN-Verbindungen zu jeder gespeicherten SSID einmalig oder täglich neu randomisiert wird.[255]

MAC-Randomisierung in Android

Android unterstützt die Randomisierung von MAC-Adressen seit der Version 6.0 „Marshmallow", die im Oktober 2015 veröffentlicht wurde. Seitdem wird die MAC-Adresse bei WLAN-Suchvorgängen zwar randomisiert, allerdings – wie bei Windows 10-Systemen – auch hier nur dann, wenn die Hardware und Treiber die Randomisierung unterstützen. Im nicht modifizierten Android Open Source Project (AOSP) wird für eine Verbindung zu Netzen, wie auch bei iOS, die echte MAC-Adresse verwendet und keine Randomisierung vorgenommen.[256] Die auf dem AOSP aufbauende Android-Distribution „CopperheadOS" wiederum bietet nach eigener Aussage eine Randomisierung der MAC-Adresse auf allen Netzwerk-Schnittstellen an (siehe Abb. 07).[257] In einem kurzen Test mit einem Nexus 5X konnte die Funktionalität der Randomisierung allerdings nur für die Mobilfunkschnittstelle bestätigt werden, während für WLAN-Verbindungen weiterhin die echte MAC-Adresse genutzt wurde.

Abb. 07 Einstellungen zur MAC-Randomisierung in CopperheadOS

Mögliche technische Gegenmaßnahmen

Grenzen des Schutzes mittels MAC-Randomisierung

Um die Nutzerinnen und Nutzer vor einer Identifizierung zu schützen, ist die Randomisierung der MAC-Adresse alleine, selbst wenn sie in allen Fällen durchgeführt wird, jedoch nicht immer ausreichend. Wie aktuelle Forschungen zeigen, können Endgeräte auch anhand von anderen Merkmalen eindeutig wiedererkannt werden.[258] So können zum einen die in den Probe Requests vorhandenen oder gerade auch nicht vorhandenen Informationen einen einzigartigen Fingerabdruck für ein Gerät erzeugen und zum anderen kann der Inhalt bestimmter Informationen selbst wiederum eine Identifizierung bedingen. So erlaubt die in manchen Probe Requests enthaltene WPS UUID (Universally Unique Identifier) einen direkten Rückschluss auf die echte MAC-Adresse, da diese als Grundlage zur Berechnung der WPS UUID dient. Zudem können Geräte, deren Probe Requests die zu findenden SSIDs enthalten, was sowohl bei älteren Geräten als auch bei solchen mit gespeicherten versteckten WLANs der Fall ist, unter Umständen anhand ihrer möglicherweise eindeutigen Kombination aus hinterlegten WLANs identifiziert werden. Im Falle von mehreren Geräten mit demselben Fingerabdruck kann ein Algorithmus zur Unterscheidung der einzelnen Geräte die Vorhersagbarkeit der Sequenznummern der Probe Requests nutzen, da diese bei den getesteten Betriebssystemen trotz eingeschalteter MAC-Randomisierung auf einem auf jedem Gerät inkrementell erhöhten Zähler beruhen.

5.2 Sicherheitsstandards und -Protokolle für 802.11 Funknetzwerke

5.2.1 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) ist ein Sicherheitsprotokoll des IEEE 802.11-Standards. WEP basiert auf dem RC4-Verschlüsselungsalgorithmus und zielte bei der Einführung darauf ab, sowohl die Vertraulichkeit und Integrität der Datenübertragung zwischen WLAN-Client und AP als auch die Benutzerauthentifizierung zu gewährleisten.

Inzwischen gilt WEP jedoch aufgrund gravierender Designfehler im Protokoll (z. B. keine Aktualisierung des Initialisierungsvektors, Integritätsüberprüfung mittels CRC32 – eine Fehlererkennungsmethode)[259] als unsicher und wurde von WPA (Wi-Fi Protected Access)[260] abgelöst, das im Folgenden vorgestellt wird.

5.2.2 Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2)-Personal

Um den Schwachstellen in WEP und den Sicherheitslücken im 802.11-Standard entgegenzuwirken, veröffentlichte die Herstellervereinigung Wi-Fi Alliance[261] im April 2003 das WPA-Protokoll. Im Jahr 2004 schlug die Standardisierungsorganisation IEEE den neuen Sicherheitsstandard 802.11i vor, der auch als WPA2 bekannt ist. WPA2 stellt eine Erweiterung des WPA-Protokolls dar, welches von Anfang an als Zwischenlösung beim Übergang von WEP zu einem besseren System galt. WPA/WPA2 ermöglicht eine Authentifizierung der Nutzerinnen und Nutzer sowie eine Verschlüsselung der WLAN-Kommunikation. Dabei bauen WPA als auch WPA2 grundsätzlich auf den Stärken des WEP-Protokolls auf und verbessern diese indem der Initialisierungsvektor für die Blockchiffrierung länger ist und für jedes Datenpaket ein neuer Schlüssel verwendet wird. Anders als bei einer einfachen Fehlererkennungsmethode wird der Schutz der Integrität durch das Message Integrity Check-Verfahren (MIC) deutlich erhöht. Während WPA zuvor auf das weniger sichere Temporal Key Integrity Protocol (TKIP) setze, um die Kommunikation zwischen WLAN-Client und AP abzusichern, wird diese bei WPA2 unter Verwendung des sog. *pre-shared key-Verfahrens* (PSK) und mit Hilfe des fortschrittlichen Verschlüsselungsverfahrens Advanced Encryption Standard (AES) gesichert. Konkret wird beim Verbindungsaufbau aus der PSK ein Sitzungsschlüssel abgeleitet der für die Verschlüsselung der WLAN-Kommunikation zwischen AP und dem Endgerät der

Nutzenden verwendet wird. Ein PSK ist in der Regel ein Passwort, das ausschließlich berechtigten WLAN-Clients zur Verfügung steht und mit dem sie sich gegenüber dem WLAN-AP authentifizieren können. Die Authentifizierung über die PSK wird meist in kleineren Netzwerken wie Heimnetzen umgesetzt. Die hierbei eingesetzte Variante von WPA2 wird dementsprechend als WPA2-Personal bezeichnet. Für den Betrieb eines öffentlichen WLANs in kleineren Geschäften und Läden (z. B. Cafés) stellt der WPA2-Personal-Modus eine attraktive Lösung dar, da der Aufwand für das Einrichten und die Wartung des Netzes ähnlich niedrig ist wie im Fall eines Heimnetzes. Um den Besucherinnen und Besuchern oder der Kundschaft einen Internetzugang über das eigene WLAN zu ermöglichen, muss ein WLAN-Betreiber allerdings allen Teilnehmenden – und somit auch potentiellen Angreifern - die korrekte PSK zur Verfügung stellen. Für Angreifer, die dadurch Teil des Funknetzes werden, ist das Abhören der Kommunikation zwischen anderen WLAN-Nutzenden und den AP ohne große Mühe möglich. Darüber hinaus ist in einem öffentlichen WLAN mit WPA2-Personal die Einrichtung eines Evil Twins möglich, da die PSK öffentlich bekannt gemacht werden muss und nur eine Authentifizierung der Nutzenden gegenüber dem AP stattfindet. Angreifer können sich dadurch den PSK auf demselben Weg wie alle anderen Nutzenden besorgen und eine Kopie des legitimen WLAN-APs einrichten. Aus diesen Gründen ist somit auch WPA2-Personal keine sinnvolle Möglichkeit, um effektive Datensicherheit und Privatheitsschutz in öffentlichen WLANs zu gewährleisten.

5.2.3 Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2)-Enterprise

Eine weitere Variante des WPA-Protokolls stellt die unter der Bezeichnung WPA2-Enterprise bekannte dar. WPA2-Enterprise ist speziell für den Einsatz in größeren WLAN-Infrastrukturen, mit mehreren und weit verteilten APs, wie z. B. für Drahtlosnetze in Unternehmen, die sich über zahlreiche Stockwerke und mehrere hundert Quadratmeter verteilen können, entworfen worden. WPA2-Enterprise bietet, ähnlich wie WPA2-Personal, eine Authentifizierung sowie eine Verschlüsselung der WLAN-Kommunikation zwischen Clients und AP an. Im WPA2-Enterprise-Modus ist die Authentifizierung der WLAN-Clients typischerweise zertifikatsbasiert (EAP-TLS Authentisierung) und wird mittels eines Authentifizierungsservers (z. B. RADIUS-Server[262]) abgewickelt. Hier authentifiziert sich der WLAN-Client entweder über einen Benutzernamen und ein Passwort und/oder mit digitalen Zertifikaten. Häufig wird die WLAN-Infrastruktur so konfiguriert, dass eine Authentifizierung des Authentifizierungsservers gegenüber dem Endgerät des Nutzers ebenfalls möglich ist. Hierbei wird ein digitales Zertifikat des Authentifizierungsservers eingesetzt, welches, je nach technischer Umsetzung, von WLAN-Clients auf ihre Gültigkeit hin überprüft werden kann. WPA2-Enterprise berücksichtigt allerdings ausschließlich die Rahmenbedingungen in großen Unternehmens-, Geschäfts- und Regierungs- bzw. Verwaltungsumgebungen, wie z. B. die vorhandene Expertise und finanziellen Ressourcen, um Authentifizierungsserver sorgfältig einzurichten und (häufig ausgehend von einer zentralen und fachkundigen Stelle) zu warten. Mit dem WPA-Enterprise-Modus ist damit theoretisch ein hohes Maß an Datensicherheit möglich, sodass die Gefahr eines Evil Twin-Angriffs als relativ niedrig eingestuft werden kann. Im Kontext öffentlicher WLANs bedeutet der Einsatz von WPA2-Enterprise allerdings ein hohes Maß an zusätzlichem Aufwand für den AP-Betreiber: Benutzer-Accounts müssen auf Anfrage schnell angelegt, verteilt und regelmäßig verwaltet werden. Für eine gegenseitige Authentifizierung müssen außerdem alle Endgeräte vorab mit notwendiger Software und Berechtigungsnachweisen (englisch *Credentials*) vorkonfiguriert werden. Des Weiteren ist die Gültigkeit des Zertifikats für Nutzende nur schwer zu validieren, wodurch ein Angriff mittels Zertifikatsfälschung möglich wird, um dennoch einen Evil Twin erfolgreich in das öffentliche WLAN zu installieren und somit den Datenverkehr abzugreifen bzw. zu manipulieren. Trotz der Vorteile ist der WPA2-Enterprise-Modus somit jedoch ebenfalls keine ausreichend praktikable und alltagstaugliche Möglichkeit für mehr Datensicherheit und -schutz in öffentlichen WLANs.

5.3 Sicherheitsstandards und -Protokolle aus dem Web-Bereich

In WLANs findet der Datenaustausch zwischen WLAN-Clients und Onlinediensten häufig unverschlüsselt statt. Sicherheitsstandards wie WPA2-Personal und WPA2-Enterprise ermöglichen den Schutz der Datenübertragung ausschließlich bis zum legitimen WLAN-AP. Am AP werden die Datenpakete dann entschlüsselt und häufig ungeschützt zum Server des Onlinedienstes weitergeleitet. Die Bedrohung der Vertraulichkeit und Authentizität der übertragenen Daten geht dabei insbesondere von MITM-, also Mittelsmann-Angriffen einerseits und Evil Twin-Angriffen andererseits aus. Dabei kann ein MITM-Angriff im gleichen Netzwerk sowohl von professionellen oder Hobby-Hackern bzw. -Hackerinnen ausgehen, als auch von ISPs bzw. WLAN-Betreibenden wie Kaufhäusern, Cafés und Behörden. Zum Schutz vor dieser Art von Attacken muss die gesamte Verbindung zwischen WLAN-Clients und Onlinediensten verschlüsselt und die Identität bzw. Authentizität beider Kommunikationspartner verifiziert werden.

5.3.1 Transport Layer Security (TLS)

Mittels TLS – Transport Layer Security (deutsch. Transportschichtsicherheit) steht den Betreibern von Webdiensten bzw. Webseiten ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet zur Verfügung.[263] Mittels TLS ist dabei die Authentifizierung des Servers und der Nutzenden möglich und damit die Gewährleitung der Integrität und Vertraulichkeit von Daten. Die Vorgängerbezeichnung von TLS ist SSL (Secure Socket Layer). Seit Version 3.0 wird das SSL Protokoll als TLS bezeichnet. TLS arbeitet auf der Transportschicht und wird von manchen Protokollen der Anwendungsschicht, wie z. B. von HTTPS oder FTPS, verwendet. Hier wird zwischen dem WLAN-Endgerät der Nutzenden und dem besuchten Server ein Verschlüsselungsschlüssel ausgetauscht und dazu verwendet, die Kommunikation zu sichern. Die verschlüsselten Daten können dann nur noch vom Web-Browser des Endgeräts oder vom Server des verwendeten Onlinedienstes entschlüsselt und gelesen werden. Da die Verschlüsselung erst ab der Transportschicht erfolgt, bleiben Metadaten wie z. B. die Netzwerkadressen der Nutzerinnen und Nutzer allerdings unverschlüsselt. Um zu gewährleisten, dass die Nutzenden mit dem Server des Onlinedienstes und nicht mit Angreifern, die sich dazwischengeschaltet haben, kommunizieren, werden Zertifikate eingesetzt. Dabei wird von einer Zertifizierungsstelle (diese werden als sogenannte vertrauenswürdige dritte Parteien bezeichnet) ein Zertifikat für den Betreiber des Servers ausgestellt. Je nach Onlinedienst ist das Zertifikat bereits Bestandteil des verwendeten Web-Browsers oder es wird bei Bedarf aus dem Internet bezogen. Dabei werden den Nutzenden Informationen über das bezogene Zertifikat angezeigt, die diese bestätigen müssen. Eine erfolgreiche Authentifizierung des Servers mittels eines Zertifikats, wird im verwendeten Web-Browser erkenntlich gemacht: Der Firefox Browser verwendet hierfür z. B. ein grünes Schloss links neben dem Adresseingabefenster.

Davon, dass die breite Masse der Nutzenden die Gültigkeit von derartigen Zertifikaten überprüft oder dass überhaupt darauf geachtet wird, dass die Kommunikation mittels TLS geschützt ist, kann jedoch nicht ausgegangen werden. Indem ein MITM-Angreifer ein gefälschtes Zertifikat erzeugt, wofür dieser z. B. BurpProxy[264] verwenden kann und das gefälschte Zertifikat vom Nutzer bzw. von der Nutzerin angenommen wird, kann ein Mittelsmann-Angriff erfolgen. Dabei wird die TLS-Verbindung zwischen dem Nutzerendgerät und dem MITM-Angreifer aufgebaut und nicht mit dem Server des gewünschten Onlinedienstes wodurch dem MITM-Angreifer ermöglicht wird, die versendeten Daten selbst zu entschlüsseln.

Ein Angriff kann auch erfolgen, wenn Nutzenden mittels SSLstrip[265] vorgetäuscht wird, dass der Server kein TLS unterstützt. Sofern das Fehlen einer TLS-Verbindung und etwaige Warnmeldungen (bspw. im Firefox Web-Browser) missachtet werden, kann wiede-

rum ein Evil Twin-Angreifer die unverschlüsselt versendeten Daten abgreifen und nach Belieben manipulieren.[266]

5.3.2 Virtuelles privates Netzwerk (VPN)

Ein gewisses Maß an Schutz ihrer Daten können WLAN-Nutzende über die Verwendung eines sog virtuellen privaten Netzwerks (VPN) genießen.[267] Bei einem VPN wird ein Tunnel zwischen zwei Netzwerkgeräten eingerichtet, um die Daten auf sichere Weise durch ein potentiell unsicheres Netzwerk, wie es z. B. in öffentlichen WLANs der Fall ist, zu leiten.[268] Dies geschieht, indem die Daten vom Tunnelanfang (Nutzerendgerät) bis hin zum Tunnelende (VPN-Server) verschlüsselt sind und von anderen Teilnehmenden des Netzwerks (z. B. des öffentlichen WLANs) nicht entschlüsselt und gelesen werden können. VPN-Server können entweder von Nutzenden selbst eingerichtet werden und Teil des Heimnetzwerks sein oder von Dritten (sowohl kostenlos als auch gegen Gebühr) angeboten werden. Datenpakete, die ins Internet geschickt werden sollen, werden dabei auf dem Endgerät, das mit dem öffentlichen WLAN verbunden ist, verschlüsselt und zunächst bis zum VPN-Server übertragen. Erst bei Erreichen des Tunnelendes, also des VPN-Servers, werden diese verschlüsselten Daten entschlüsselt und über das Internet zum Onlinedienst weitergeleitet (Vgl. Abb. 08).

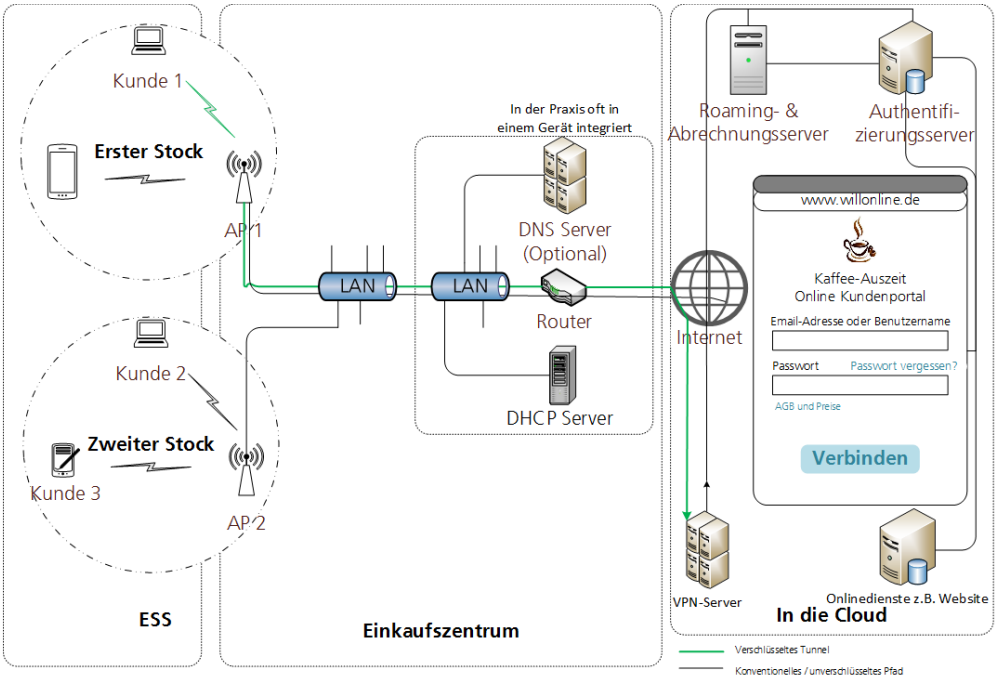

Abb. 08 Vereinfache Darstellung eines VPN-Tunnels in einem öffentlichen Netzwerk. Mit Hilfe einer VPN-App im Nutzerendgerät wird ein Tunnel (Grün eingezeichnet) zum VPN-Server aufgebaut, durch den Daten verschlüsselt übertragen werden. Beim VPN-Server endet der Tunnel. Dort werden die Daten entschlüsselt und zum gewünschten Onlinedienst weitergeleitet.

Bei virtuellen privaten Netzwerken kann zwischen VPN-Lösungen auf Basis von SSL/TLS und IP-basierten VPN-Tools unterschieden werden. Grundsätzlich bieten VPN-Techniken, sofern richtig implementiert und konfiguriert, einen effektiven Schutz gegen Angriffe wie das passive Abhören, Evil Twin-Angriffe und gefälschte WLAN-APs, die im öffentlichen WLANs erfolgen können. Zwar ist dabei eine Erkennung der Angreifer nicht möglich, allerdings wird mittels Verschlüsselung die Beeinträchtigung der Vertraulichkeit und Integrität des Datenaustauschs verhindert. Mit VPNs findet zudem eine Authentifizierung der Endgeräte z. B. durch ein digitales Zertifikat statt.

Allerdings kann VPN dennoch nicht als eine ideale Möglichkeit des (Selbst-)Datenschutzes angesehen werden.[269] Die Konfiguration eines VPN-Tools und die Wartung eines VPN-Servers sind für viele Nutzende zu aufwändig, weshalb VPNs als Schutzmöglichkeit kaum zur Verwendung kommen. In Deutschland machen VPN-Verbindungen nur 16% des gesamten Internetverkehrs aus.[270] Zudem werden VPN-Tools, sofern sie eingesetzt werden, oft nicht entsprechend der erforderlichen Sicherheitsrichtlinien konfiguriert oder mit fehlerhaften Voreinstellungen verwendet. Eine fehlerhafte Implementierung bzw. Konfiguration kann es Angreifern erlauben, die On-

Mögliche technische Gegenmaßnahmen

line-Aktivitäten der Nutzenden öffentlicher WLANs unbemerkt zu protokollieren.[271] Auch Angriffe auf Basis gefälschter SSL/TLS-Zertifikate, wie sie in Abschnitt 5.3.1 vorgestellt wurden, können hier stattfinden. Darüber hinaus besteht die Möglichkeit, dass der VPN-Server, aufgrund seiner Vermittlerrolle zwischen Online-Diensten und mit diesen verbundenen Nutzerendgeräten, selbst als MITM-Komponente eingesetzt wird. Folglich ist die Verwendung von VPN-Tools lediglich eine Verschiebung des Vertrauens von einem Vermittler (WLAN-Router) zum anderen (VPN-Server). Dementsprechend müssen Nutzende von VPN-Tools den Betreibern der VPN-Server (also entweder Drittanbietern oder dem eigenen Können beim Aufbau und Betrieb) stets vertrauen. Abhilfe könnte die Möglichkeit schaffen, den heimischen WLAN-Router als VPN-Server einzurichten.[272] Eine Alternative zum VPN stellt die Software Tor (das Browser-Paket bzw. die Tor-App und das dezentrale Tor-Netzwerk) dar. Anders als mit VPN findet die Datenübertragung mittels Tor nicht über einen einzelnen, kompromittierbaren Vermittler (VPN-Server), sondern gleich über mehrere, dezentral verteilte *Vermittler* (die sog. *Tor-Server-Archjtektur*) statt.[273] Mit Tor können somit WLAN-Nutzende anonymer im Internet unterwegs sein als VPN-Nutzende.[274]

5.4 Erkennungsmöglichkeiten von Evil Twins

Neben den oben beschriebenen Standards und Protokollen existiert eine wachsende Anzahl von Vorschlägen, die explizit drauf abzielen, Evil Twin-APs zu erkennen und so mögliche Bedrohungen für IT-Sicherheit und Datenschutz frühzeitig zu unterbinden. Derartige Erkennungsmethoden sind jedoch i. d. R. Vorschläge aus der Wissenschaft, die bislang kaum in der Praxis eingesetzt werden.

Techniken zur Erkennung von Evil Twin-APs lassen sich, je nachdem wer die Erkennung durchführt und wie das Netz aufgebaut ist, grundsätzlich in zwei Hauptkategorien einteilen: Schutzmöglichkeiten vor Evil Twins aus Betreibersicht[275] und Schutzmöglichkeiten vor Evil Twins aus Nutzersicht.[276] Beide Erkennungsmethoden basieren auf dem Einsatz eines sog. Fingerprints (deutsch *Fingerabdruck*) des APs. Ein Fingerprint stellt ein eindeutiges Identifizierungsmerkmal des APs dar und kann entweder aus Details über das Funksignal (z. B. Änderungen der Signalstärke des APs oder des Zustands des Kommunikationskanals),[277] aus physikalischen Merkmalen des WLAN-Routers[278] oder aus Informationen wie der IP-Adresse und des Standort des APs und aus Details über den ISP[279] gewonnen werden. Andere Erkennungsmöglichkeiten zielen explizit auf die Erkennung von Software-basierten Evil Twin-APs[280] oder auf eine Modifizierung der 802.11-Norm und -Protokolle ab.[281]

Mit den hier aufgelisteten Schutzmöglichkeiten können einzelne Evil Twin-Angriffe schnell und z. T. effektiv erkannt werden. In der Praxis verfügen Angreifer jedoch über eine Vielzahl von Optionen um Software- bzw. Hardware-basierte Evil Twins-APs zu betreiben. Die Kombination dieser Erkennungsansätze zu einem holistischen Rahmenwerk für den Schutz der Privatheit in öffentlichen WLANs gilt als vielversprechender Ansatz, stellt Forschung und Entwicklung jedoch gegenwärtig noch vor erhebliche Herausforderungen.

6
Anregung einer öffentlichen Debatte über Internetzugang als Grundversorgung

In verschiedenen Debatten, insbesondere bezüglich der Netzneutralität, ist Internet als öffentliches Gut thematisiert worden – anfänglich vor allem aus dem Bereich des Netzaktivismus und NGOs im Bereich Bürgerrechte.[282] Aber auch ganz grundsätzlich kann eine umfassende Bereitstellung von Internetdiensten das Ansehen oder das soziale Klima verändern. Unabhängig von den Details der Realisierung hat es z. B. Estland geschafft, sich als weltoffenes, technikaffines Land zu positionieren. Dazu gehört auch die Auffassung, der Zugang zum Internet sei ein Bürgerrecht.[283] Auch andere Staats- und Regierungschefs haben die Rede vom Internet als öffentlichem Gut aufgegriffen.[284] Mit einem einfachen, möglichst freien Zugang zum Internet über öffentliche WLANs wird aber nicht nur ein öffentliches Gut im emphatischen Sinn beschrieben. Vielerlei Interessenten sehen darin ganz konkrete Verbesserungen der wirtschaftlichen Bedingungen. Im Fall des öffentlichen Internetzugangs in Bars, Cafés, Hotels und dergleichen betrifft das zuerst die Betreiber dieser Einrichtungen. Sie können Ihrer Kundschaft einen zusätzlichen Service bieten, welcher den eigenen Betrieb attraktiver macht. Gleichzeitig kann die verbreitete Verfügbarkeit solcher Zugänge sich bspw. auch vorteilhaft auf den Tourismus auswirken. Ein attraktiver Ort für digitale Nomaden und Startup-Kultur zu sein, ist ein weiteres Ziel, das Kommunen wie z. B. Berlin auch strategisch verfolgen. Hier trifft sich das Interesse der Stadt bis zu einem gewissen Grade mit den Partikularinteressen von Gastronomie, Hotels, etc.

Derlei WLAN-Angebote werden oftmals als *Freies WLAN* oder auch als *Free Wi-Fi* beworben. Gleichzeitig ist die Nutzung von öffentlichen WLANs nicht wirklich frei. Die Anbieter der Zugänge kaufen diese bei Telekommunikationsunternehmen oder anderen Dienstleistern, welche über vielfältige Möglichkeiten der Datenauswertung verfügen. Inzwischen bieten Telekommunikationsdienstleister auch direkt Pakete an, um im öffentlichen Raum Internetzugang einzurichten. Auch hier fallen wertvolle Daten bei den Unternehmen an. Wenn ein Unternehmen eine ganze Stadt oder sogar in ganz Deutschland eine Vielzahl von Zugangspunkten anbietet, können Nutzerinnen und Nutzer darüber identifiziert und verfolgt werden. Auch größere gewerbliche Anbieter von öffentlichen Zugangspunkten wie Café- oder Fast-Food-Ketten haben diese Möglichkeit. Das heißt auch hier bedeutet „frei" nicht wirklich „kostenlos", vielmehr wird zahlungsfreier Zugang im Zweifelsfall durch Auswirkungen auf die Privatheit „erkauft".

Angesichts der oben genannten Vorteile für private Betreiber, Kommunen und dem Wert des Internetzugangs als öffentliches Gut, stellt sich die Frage, ob dies ein angemessener „Preis" für Internetzugang sein mag. Im Falle offener WLANs in kommerziell betriebenen Kontexten verdienen z. B. die Betreiber einer Bar am Konsum der Kundinnen und Kunden. Davon wiederum wird der kostenpflichtig gekaufte Zugang beim Telekommunikationsbetreiber erworben. Damit wäre der Zugang bereits bezahlt, was die Rechtfertigung zusätzlicher Einnahmen durch Datenauswertung erschwert. Die Praxis der Datenauswertung durch WLAN-Betreibende in anderen Ländern verdeutlicht erneut, dass Akteure aus der Wirtschaft zugunsten der eigenen Mehrwertmaximierung ein privatheitsgefährdendes Verhalten an den Tag legen. Freilich wird dabei versucht, die Datenauswertung auch für die Kunden gleichermaßen profitabel erscheinen zu lassen, indem diese bspw. auf Basis von *in store location tracking* – also der Standortbestimmung innerhalb eines Geschäfts – an Sonderangebote herangeführt werden sollen. Angesichts der sich noch weiter ausweitenden Datenmacht gewerblicher Akteure kann allerdings bezweifelt werden, in welchem Verhältnis der (behauptete) Kundennutzen zu dem Nutzen steht, der privaten Unternehmen zuteilwird.

Anregung einer öffentlichen Debatte über Internetzugang als Grundversorgung

Im Fall von Kommunen oder anderen Einrichtungen der öffentlichen Hand stellt sich die Frage, ob die Bereitstellung von öffentlichem WLAN nur eine angenehme Zusatzleistung ist, von der aber durchaus erwartet werden kann, dass die Nutzerinnen und Nutzer dafür wenigstens indirekt etwas leisten (z. B. durch Nutzung ihrer Daten) oder Werbung in Kauf nehmen müssen. Dagegen könnte man argumentieren, dass öffentlicher WLAN-Zugang tatsächlich ein Gut oder Service ist, das als so wichtig angesehen wird, dass die Kommune die Finanzierung dafür übernimmt. Die Frage, wie die Vielzahl an Geflüchteten in Europa mit Internetzugang versorgt werden kann, hat beispielsweise gezeigt, dass längst nicht alle Menschen öffentliches WLAN als Zusatzangebot auf Reisen oder Alternative zum Internet zu Hause nutzen. Für diverse Bevölkerungsgruppen ist es die einzige Möglichkeit, ins Internet zu gelangen.

Noch gar nicht ausgeschöpft sind Möglichkeiten, den Unterschied zwischen einem durch die Anbieter bezahlten und einem durch Datennutzung und Werbung finanzierten Zugang auch zu thematisieren. So wäre z. B. denkbar, dass eine Kommune oder ein Restaurant damit werben könnte, nicht einfach nur öffentliches WLAN, sondern privatheitsschonendes öffentliches WLAN einzurichten. Insbesondere die öffentliche Hand könnte dabei damit werben, dass die Nutzenden bei ihnen hohes Vertrauen in die Einhaltung von Datenschutzvorschriften haben können.

Überlegungen sollten auch berücksichtigen, dass viele Telekommunikationsdienstleister über private WLANs versuchen, ein breites Netz an Zugangspunkten anzubieten, das aber nur für die eigenen Kundinnen und Kunden zugänglich ist. Dagegen stehen Bürgerinitiativen wie das Freifunk-Netz, in dem Bürgerinnen und Bürger ihre privaten Zugänge freiwillig (und ohne finanziellen Nutzen für die Anbieter) zusammenschließen.

So wichtig die Frage danach, inwieweit eine Grundversorgung mit WLAN als öffentliches Gut gelten kann, ist, wurden im White Paper aber auch Datenschutz- und IT-Sicherheitsprobleme im Zusammenhang mit öffentlichen WLANs deutlich: Sollte die Anzahl öffentlicher WLAN-Hotspots – so wie es mit den Gesetzesänderungen im Bereich der Störerhaftung bezweckt worden ist – steigen[285] und Nutzerinnen und Nutzer sich einer Vielzahl von Netzen und Zugangspunkten gegenübersehen, werden sich die Probleme vervielfachen.

Sowohl Nutzende als auch viele Anbieter öffentlicher WLANs teilen ein starkes Interesse an einer möglichst offenen WLAN-Nutzung, die ohne Anmeldung mit Benutzernamen und Passwort auskommt. Schließlich gilt: Je umständlicher die Anmeldung bei einem öffentlichen WLAN ist, umso größer ist die Sorge, dass bspw. die Kundschaft zum Konkurrenzgeschäft abwandert, das ein einfacher zugängliches oder gar ein vollständig anmeldefreies WLAN anbietet. Ein völlig offenes WLAN bedeutet aber zugleich, dass das jeweilige WLAN unverschlüsselt und damit auch weitestgehend ungeschützt ist. Verschlüsselung (idealerweise mittels WPA2-Enterprise) allein ist zwar kein Allheilmittel gegen die geschilderten, vielfältigen IT-Sicherheits- und Datenschutzprobleme, doch bieten die in Abschnitt 5 geschilderten Maßnahmen, zu denen Verschlüsselung zählt, einen ersten Anhaltspunkt, wie den Problemen begegnet werden kann.

Uns ist klar, dass vielen Bürgerinnen und Bürgern und auch zahlreichen WLAN-Betreibern ein möglichst einfacher Zugang zum Internet über ein offenes WLAN wichtig ist, doch möchten wir gerade auch die Schattenseiten offener WLANs aufzeigen, und darüber hinaus eine öffentliche Debatte initiieren, wie sicher öffentliche WLANs verschiedener Ausprägung überhaupt sein können. Es wäre bereits viel getan, wenn sich Forschung, Hersteller und Betreiber der Sicherheitsprobleme annehmen und die Politik die Entwicklung von innovativen und effektiven Schutzmaßnahmen fördern würden.

Wünschenswert wäre insbesondere eine öffentliche Debatte darüber, inwiefern die von vielen Seiten geforderte Offenheit mit Datenschutz und -sicherheit sowie anderen rechtlichen Vorschriften in Einklang gebracht werden kann. Die Praxis, bei der Einrichtung von WLAN-Hotspots auf die Infrastruktur von Internet-Providern zugreifen zu

können, um sich der haftungsrechtlichen Probleme zu entledigen, stellt dabei nur eine Möglichkeit dar, die zudem auch nicht den Bedürfnissen aller Bürgerinnen und Bürger gerecht wird. Was ist mit jenen Personen, die ihr privates WLAN für die Nachbarn öffnen wollen? Wie lässt sich die im EuGH-Urteil geforderte Identifikation der Nutzenden mit dem Datenschutzrecht vereinbaren? Werden Freifunk-Initiativen den Datenverkehr auch weiterhin ins Ausland – wo laxere Regeln zur Störerhaftung gelten – routen müssen, um haftungsrechtlichen Schwierigkeiten aus dem Weg zu gehen? Und wie kann das Strafrecht wirksamer gestaltet werden, ohne dass daraus wiederum datenschutzrechtliche Bedenken erwachsen und ohne dass experimentelle Praktiken von unschädlichen Hackern eingeschränkt werden?

Anregung einer öffentlichen Debatte über Internetzugang als Grundversorgung

Eine Diskussion dieser Fragen unter der Ägide, öffentliches WLAN als Grundversorgung zu verstehen, ist unseres Erachtens eine sinnvolle Möglichkeit, diese und weitere Fragen zielführend anzugehen.

Anmerkungen

[1] Siehe auch: Bundesamt für Sicherheit in der Informationstechnik: LAN und WLAN sicher einrichten: Öffentliche WLANs. Online: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/FremdeWLAN/fremdeWLAN_node.html (09.02.2017); Schafroth, Florian (2012): Heiße Sicherheitstipps für Hotspots. In: Kaspersky Lab, erschienen am: 31.05.2012, http://newsroom.kaspersky.eu/de/texte/detail/article/heisse-sicherheitstipps-fuer-hotspots (09.02.2017).

[2] Der einfache Zugriff z. B. auf Online-Nachrichten, Wettervorhersagen usw. wobei vor allem Informationen aus dem Netz abgerufen und keine Anmeldeinformationen ins Netz übertragen werden, ist etwas weniger sensibel.

[3] BSI (2016): IT-Grundschutz-Kataloge, Abschnitt M 2.11 Regelung des Passwortgebrauchs. Online: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html (01.03.2017).

[4] NIST (2016): Special Publication 800-63-3: Digital Identity Guidelines. Online: https://pages.nist.gov/800-63-3/ (17.03.2017).

[5] BSI (2016): IT-Grundschutz-Kataloge, Abschnitt M4 Hardware und Software, Unterabschnitt M 4.201 - M 4.205. Online: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04.html (01.03.2017).

[6] Deutscher Bundesverband IT-Sicherheit e. V: TeleTrusT-Initiative „IT-Security made in Germany“. Online: https://www.teletrust.de/itsmig/kriterien-und-antrag/ (22.02.2017)

[7] Üblicherweise müssen sich Nutzende von öffentlichen WLAN-Angeboten einmalig registrieren und sich bei jedem Zugriff Identifizieren (bzw. dem WLAN-Anbieter einen Vertrauensnachweis erbringen). Allerdings werden häufig aufgrund ökonomischer Zwänge (z. B. die Abrechnung) und anderer Anforderungen (z. B. bzgl. der Vorratsdatenspeicherung) Benutzerkonten angelegt, Nutzeraktivitäten korreliert und einer Person eindeutig zugewiesen. Herkömmliche Ansätze für die Nutzerregistrierung und -identifizierung in der Praxis setzen daher i. d. R. die Preisgabe (sensibler) personenbezogener Daten voraus. Um den Schutz der Privatheit zu gewährleisten, sollen idealerweise nicht-verkettbare Identitäten verwendet, und nur das Minimum an persönlichen Daten verlangt werden, auf Basis dessen ein WLAN-Angebot bereitgestellt werden soll. Vielversprechende kryptographische Protokolle und Systeme, um diese Anforderungen zu erfüllen, sind in den letzten Jahrzehnten von zahlreichen europäischen und nationalen Initiativen entwickelt und vorgeschlagen worden. Allerdings lösen diese Forschungsergebnisse die aktuellen Privacy-Herausforderungen in der Praxis nur teilweise. Zum einen wurden gegenwärtige Vorschläge zur Realisierung datenminimierender Authentifikation und vertrauenswürdigem Austausch von Attributaussagen über Benutzer unter der Annahme entworfen, eine Integration in bereits in der Praxis vorhandene Identitätsmanagement-Systeme, sei mit minimalem Aufwand zu erreichen. In der Tat fordert die neue Semantik der Protokolle jedoch häufig kostspielige technische Anpassungen der eingesetzten Identitätsmanagement-Systeme. Zusätzliche Kosten aufgrund technischer Anpassungen an in der Praxis bereits bewährte Systeme (aus Sicht der Funktionalität) gelten als mögliche Hindernisse für eine breite Akzeptanz seitens der Diensteanbieter. Allerdings, sehen diese bislang keine Anreize – weder ökonomische noch rechtliche – derartige Anpassungen durchzuführen.

Zum anderen wurden Vorschläge für Systeme und Protokollfamilien aus vergangenen Forschungsinitiativen nicht darauf ausgelegt, den Schutz der Privatheit in allen Phasen des Identitätsmanagements in einer integrierenden Art und Weise zu gewährleisten. Während die Effektivität und technische Umsetzbarkeit der Vorschläge für eine selekti-

Anmerkungen

ve Datenherausgabe und domain-spezifische Pseudonyme nachgewiesen worden sind, bestehen nach wie vor ernste Bedenken hinsichtlich der Erfüllung unabdingbarer Anforderungen, wie z. B. Benutzer-Accountability (Pseudonyme werden blind signiert und die effektive Realisierung der Nicht-Abstreitbarkeit bzw. Verbindlichkeit kaum möglich) und Transparenz (was passiert mit meinen Daten). Daher besteht hier weiterer Forschungs- und Entwicklungsbedarf.

[8] Bundesministerium des Innern (2016): Cyber-Sicherheitsstrategie für Deutschland 2016. Online: https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cybersicherheitsstrategie-2016-barrierefrei.pdf?__blob=publicationFile (17.03.2017).

[9] Vgl. dazu: Simo, Hervais/Gassen, Marius (2016): Towards Privacy-preserving Mobile Location Analytics. In: Privacy and anonymity in the information society PAIS2016 - Proceedings of the Joint EDBT/ICDT 2016 Workshops, Bordeaux/France.

[10] Bundesamt für Sicherheit in der Informationstechnik (o. J.): Evaluation Assurance Level (EAL), Common Criteria. Online: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/ITSicherheitskriterien/CommonCriteria/eal_stufe.html (08.03.2017).

[11] In Anlehnung an die Vorgaben des Dudens wird im Folgenden versucht, eine sowohl gendersensible als auch gut lesbare Schreibweise umzusetzen. Das heißt, dass eine symmetrische Benennung von Frauen und Männern oder eine geschlechtsneutrale Bezeichnung praktiziert wird, wo immer dies den Lesefluss nicht beeinträchtigt. Wo eine Beeinträchtigung (bspw. aufgrund eines bereits sehr verschachtelten bzw. komplexen Satzes) nicht ohne Auswirkungen auf den Lesefluss bzw. ohne eine Verunstaltung der Sprache nicht möglich ist, wird auf die Sparschreibung mittels eines Schrägstrichs oder einer Klammer und in Einzelfällen auch auf das generische Maskulinum zurückgegriffen.

[12] Eurostat (2016): Level of Internet Access – Households. Last Update: 06.07.2016. Online: http://ec.europa.eu/eurostat/tgm/download.do?tab=table&plugin=1&language=en&pcode=tin00134 (25.07.2016); Statistisches Bundesamt (2016): Wirtschaftsrechnungen. Private Haushalte in der Informationsgesellschaft – Nutzung von Informations- und Kommunikationstechnologien. Fachserie 15 Reihe 4, korrigierte Fassung vom 03.03.2016, Wiesbaden, S. 16.

[13] NinthDecimal. (n.d.). Anzahl der öffentlichen Wi-Fi Locations und Hot Spots weltweit von 2006 bis 2013. In Statista - Das Statistik-Portal. Zugriff am 21. Juli 2016, von http://de.statista.com/statistik/daten/studie/158345/umfrage/anzahl-der-wi-fi-locations-und-hot-spots-weltweit-seit-2006/.

[14] Bitkom. (n.d.). Verfügbarkeit von WLAN-Hotspots in ausgewählten Ländern nach Anzahl je 100.000 Einwohner im Jahr 2011. In Statista - Das Statistik-Portal. Zugriff am 21. Juli 2016, von http://de.statista.com/statistik/daten/studie/165018/umfrage/verfuegbarkeit-von-wlan-hotspots-im-laendervergleich/.

[15] Eco – Verband der deutschen Internetwirtschaft e. V. (2014): Verbreitung und Nutzbarkeit von WLAN, WLAN-Zugangspunkten sowie öffentlicher Hotspots in Deutschland.

[16] Eco – Verband der deutschen Internetwirtschaft e. V. (2014).

[17] Eco – Verband der deutschen Internetwirtschaft e. V. (2014).

Anmerkungen

[18] Müller, V., Kipker, D.-K. (2016), Der Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes. Hat die Bundesregierung eine zeitgemäße Angleichung des TMG verfehlt? In: Multimedia und Recht (MMR) 2016, 87; Mantz, R., Sassenberg, T (2014a): Rechtsfragen beim Betrieb von öffentlicher WLAN-Hotspots. In: Neue Juristische Woche (NJW), Heft 49, S. 3537.

[19] Grigorjew (2016), S. 706.

[20] Dachwitz, WLAN-Störerhaftung: Große Koalition kann sich nicht zu echter Rechtssicherheit für offene Netze durchringen, Netzpolitik.org. vom 31.5.2016, https://netzpolitik.org/2016/wlan-stoererhaftung-grosse-koalition-kann-sich-nicht-zu-echter-rechtssicherheit-fuer-offene-netze-durchringen/. Siehe dazu auch Müller, V., Kipker, D.-K. (2016).

[21] Dörner, Stephan (2016): Deutschland blamiert sich als WLAN-Wüste. Die Welt vom 16.03.2016. Online: http://www.welt.de/wirtschaft/webwelt/article153354781/Deutschland-blamiert-sich-als-WLAN-Wueste.html (27.07.2016).

[22] BT-Drs. 18/8645 vom 1.6.2016, S. 7; Grigorjew (2016), S. 701.

[23] Dhir, Amit. "Wireless Home Networks—DECT, Bluetooth, HomeRF, and Wireless LANs." Xilinx, White Paper 135 (2001).

[24] Die Einstiegsseite ist jene Seite, die automatisch aufgerufen wird, sobald eine WLAN-Verbindung mit einem (öffentlichen) WLAN hergestellt wird und auf der grundlegende Informationen zum Netzwerk bereitgestellt werden (z. B. in Form von Nutzungsbedingungen). Je nach WLAN-Typ bzw. -Anbieter sind auf der Einstiegsseite weitere Schritte erforderlich, bevor auf das Internet zugegriffen werden kann: Bei einigen Anbietern ist vor der Nutzung des WLANs zudem eine Anmeldung mit Benutzername und Kennwort auf der Einstiegsseite erforderlich (etwa bei den WLAN-Hotspots von Telekommunikationsdienstleistern oder in Hotels usw.). In anderen Fällen müssen lediglich die Nutzungsbedingungen akzeptiert werden, bevor das WLAN genutzt werden kann (z. B. in den WLANs der Deutschen Bahn) oder die Nutzerinnen und Nutzer werden über nahegelegene (touristische, kulinarische usw.) Angebote informiert (etwa in öffentlich betriebenen WLANs).

[25] In den Zügen der Deutschen Bahn AG wiederum funktioniert die Identifizierung.

[26] I. d. R. fallen auch firmeneigene WLANs in diese Kategorie, da sie nur für ausgewählte Personenkreise angeboten und primär für betriebliche Zwecke eingesetzt werden.

[27] IEEE Standard Association. IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY). 2012.

[28] Professionelle Netze meint hier solche, die von gewerblichen und kommunalen Akteuren betrieben und angeboten werden.

[29] Datenpakete werden vom AP aus an alle Geräte die sich innerhalb seiner Funkreichweite befinden übertragen.

[30] Bereits bei der Herstellung eines Gerätes mit Netzwerkfunktionen wird seitens des Herstellers jeder Netzwerkschnittstelle eine eindeutige MAC-Adresse zugewiesen, die dann als Netzwerkadresse für jede Kommunikation auf Data-Link-Ebene genutzt wird.

[31] Berlin.de (2016): Projekt "Free WiFi Berlin". Online: https://www.berlin.de/rbmskzl/medien/netzpolitik/wlan-projekt/projekt-free-wifi-berlin-32144.php (30.11.2016).

[32] Südwest Presse (2015a): Vier kostenlose Wlan-Hotsports für Ulm freigeschaltet. Online: http://www.swp.de/ulm/lokales/ulm_neu_ulm/Vier-kostenlose-Wlan-Hotspots-fuer-Ulm-freigeschaltet;art1158544,3527015 (30.11.2016).

[33] Südwest Presse (2016): Öffentliches WLAN zieht Touristen an. Online: http://www.swp.de/ulm/nachrichten/suedwestumschau/Oeffentliches-WLAN-nbsp-zieht-Touristen-an;art1222894,3909523 (30.11.2016).

[34] Vgl. Südwest Presse (2015a).

[35] Vgl. Südwest Presse (2016).

[36] Akosim (2015); Fraser (2009); Farkas et al. (2009); Tapia, Maitland, Stone (2006); Bar and Park (2006); Oliver et al (2010).

[37] muenster.de (2015): Freies WLAN für Flüchtlingseinrichtungen. Online: http://www.muenster.de/stadt/presseservice/pressemeldungen/web/frontend/show/912660 (30.11.2016).

[38] Tapia, Maitland, Stone (2006); Freifunk Kassel (2015): Pro und Contra Freifunk. Online: https://freifunk-kassel.de/Pro%20und%20Contra (30.11.2016)

[39] saarbruecken.de (2016): Saarbrücken mit der App erleben- für Android und iOS. Online: http://www.saarbruecken.de/rathaus/presse_und_online/saarbruecken_app (30.11.2016).

[40] Akosim (2015); Mandviwalla et al. (2008).

[41] Blumenfeld (2008).

[42] muenchen.de (2016): Die München App für Android, iPhone und iPad. Online: http://www.muenchen.de/meta/iphone-android-app.html (30.11.2016).

[43] audible (2016): Free WIFI Berlin: Das Projekt "Free WiFi Berlin" versorgt die deutsche Hauptstadt mit kostenlosem WLAN. Online: http://www.hoerbuecher-blog.de/wifi/ (30.11.2016)

[44] Telespiegel (2016); Mahler und Steinfield (2003); Campbell, Anita (2014): Study: Yes, there are benefits of offering free WiFi. In: SmallBusiness Trends. Online: http://smallbiztrends.com/2014/06/benefits-of-offering-free-wifi.html (30.11.2016).

[45] Campbell (2014).

[46] Yusop et al (2010); Business Time Zone Global Info (2016); My Place Connect (2016)

[47] Deloitte Consumer Survey (2010).

[48] Deloitte consumer survey (2010).

[49] Moore, Michael (2014): Tesco Shoppers to get free In-Store BT Wi-Fi. In: TechWeek Europe. Online: http://www.techweekeurope.co.uk/workspace/tesco-bt-instore-wifi-156016 (30.11.2016).

[50] Vella, Matt (2012): Why stores are finally turning on to WiFi. In: Fortune. Online: http://fortune.com/2012/12/14/why-stores-are-finally-turning-on-to-wifi/ (30.11.2016).

[51] Subramanian, Gopalaratnam (2015): In-store analytics: tracking real-world customer just like online shoppers- Using Wi-Fi, video cameras and more. Online: http://www.techradar.com/news/world-of-tech/future-tech/in-store-analytics-tracking-real-world-customers-just-like-online-shoppers-1286293 (30.11.2016).

[52] Graham, Charlton (2012): Should retailers offer in-store wi-fi?. In: Econsultancy. Online: https://econsultancy.com/blog/11148-should-retailers-offer-in-store-wi-fi/ (30.11.2016).

[53] Deloitte consumer survey (2010); My Place Connect (2016).

[54] Vgl. Vella (2012).

[55] Telespiegel.de (2016): WLAN-Hotspots- kostenlose Wi-Fi an öffentlichen Plätzen. Online: http://www.telespiegel.de/internet/wlan-hotspots.php (30.11.2016).

Anmerkungen

[56] Basierend auf den verschiedenen Vorteilen, die sich für die einzelnen Zielgruppen ergeben können, gibt es auch bei der Nutzung des WLANs Unterschiede. Die Studienergebnisse der Stadt Lugano zeigen, dass private Nutzende das frei verfügbare WLAN zumeist für das Versenden von Nachrichten über E-Mails oder Sofortnachrichtendienste nutzen, während Geschäftsleute daneben auch andere Anwendungen im Browser verwenden. Touristen greifen dagegen eher auf spezielle Touristeninformationen und soziale Netzwerkplattformen zu. Typische Freizeitnutzer/-innen verwenden das angebotene WLAN zumeist zum Lesen und Schreiben von E-Mails und zum Austausch über soziale Netzwerkplattformen. Dabei wird am häufigsten vom Smartphone aus auf das WLAN zugegriffen, nur bei Geschäftsleuten ist der Laptop eine häufig genutzte Zugangsquelle. Vgl. Picco-Schwendener et al. (2015): Tourists and Municipal Wi-Fi Networks (MWN): The Case of Lugano (Switzerland).

[57] DM (2016): Das DM Kunden WLAN. Online: https://www.dm.de/services/services-im-markt/das-dm-kunden-wlan/ (30.11.2016).

[58] Deloitte consumer survey (2010).

[59] Hampton und Gupta (2008).

[60] Mandviwalla et al (2008).

[61] Bundesamt für Sicherheit in der Informationstechnik, Informationssicherheit und IT-Grundschutz: BSI-Standards 100-1 bis 100-3. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html (01.03.2017).

[62] Wallace, B. (2015): Vulnerability: CVE-2015-0932, erschienen am: 26.03.2015, https://blog.cylance.com/spear-team-cve-2015-0932 (03.03.2017); Kim, P. (2016): Security vulnerabilities in the D-Link DWR-932B LTE router, erschienen am: 28.09.2016, https://pierrekim.github.io/blog/2016-09-28-dlink-dwr-932b-lte-routers-vulnerabilities.html (28.09.2016); Checkoway, S., Cohney, S., Garman, C.; Green, M.; Heninger, N., Maskiewicz, J., Rescorla, E., Shacham, H., Weinmann, R.-P. (2016): A Systematic Analysis of the Juniper Dual EC Incident. Cryptology ePrint Archive, Report 2016/376.

[63] Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015): Unlocking the Potential of the Internet of Things. In: McKinsey Global Institute, erschienen im: Juni 2015, http://goo.gl/qzq5mV (01.12.2016).

[64] A. B. M. Musa and Jakob Eriksson (2012): Tracking unmodified smartphones using Wi-Fi monitors. In ACM SenSys'12; Cuthbert Daniel and Wilkinson Glenn (2012): Snoopy: Distributed tracking and profiling framework. In 44Con 2012; Simo und Gassen (2016).

[65] Lindqvist, Janne; Tuomas Aura; Danezis, George; Koponen, Teemu; Myllyniemi, Annu; Mäki, Jussi and Michael Roe (2009): Privacy-preserving 802.11 access-point discovery. In: ACM WiSec, 2009; Greenstein, Ben; Gummadi, Ramakrishna; Pang, Jeffrey; Chen, Mike Y.; Kohno, Tadayoshi; Seshan, Srinivasan and David Wetherall (2007): Can Ferris Bueller still have his day off? protecting privacy in the wireless era. In: USENIX HotOS workshop, 2007.

[66] Cunche, M., Kaafar, M. A. Kaafar, and R. Boreli (2012): I know who you will meet this evening! linking wireless devices using wi-fi probe requests. In: World of Wireless, Mobile and Multimedia Networks, 2012 IEEE International Symposium on a. IEEE, pp. 19.

[67] Mayer, J., Mutchler, P., & Mitchell, J. C. (2016). Evaluating the privacy properties of telephone metadata. Proceedings of the National Academy of Sciences, 113(20), 5536-5541.

[68] Tews, Erik and Martin Beck (2009): Practical attacks against WEP and WPA. In: Proceedings of the second ACM conference on Wireless network security. ACM, 2009, pp. 79-86.

[69] Checkoway, Stephen; Cohney, Shaanan; Garman, Christina; Green, Matthew; Heninger, Nadia; Maskiewicz, Jacob; Rescorla, Eric; Shacham, Hovav; Weinmann, Ralf-Philipp (2016): A Systematic Analysis of the Juniper Dual EC Incident. Cryptology ePrint Archive, Report 2016/376.

[70] Scherschel F. (2016): Telekom-Störung: BSI warnt vor weltweitem Hackerangriff auf DSL-Modems. In: Heise Security, erschienen am: 28.11.2016, https://www.heise.de/security/meldung/Telekom-Stoerung-BSI-warnt-vor-weltweitem-Hackerangriff-auf-DSL-Modems-3506556.html (03.03.2017).

[71] Sivakorn, Suphannee; Iasonas Polakis, and Angelos D. Keromytis (2016): The Cracked Cookie Jar: HTTP Cookie Hijacking and the Exposure of Private Information.; Vgl. Tews; Beck (2009).

[72] Sivakorn, Suphannee, Jason Polakis, and Angelos D. Keromytis. "HTTP Cookie Hijacking in the Wild: Security and Privacy Implications."

[73] Ullrich, J. (2016). Port 7547 SOAP Remote Code Execution Attack Against DSL Modems. In: SANS Internet Storm Center, erschienen am: 29.11.2016, https://isc.sans.edu/forums/diary/Port+7547+SOAP+Remote+Code+Execution+Attack+Against+DSL+Modems/21759/ (03.03.2017).

[74] A. Dabrowski, G. Merzdovnik, N. Kommenda, and E. Weippl, "Browser history stealing with captive wi-fi portals," in Proceedings of Workshops at IEEE Security and Privacy 2016, Mobile Security Technologies (MoST), 2016; OWASP, T. (2013). 10: Ten Most Critical Web Application Security Risks.

[75] Vgl. Tews; Beck (2009).

[76] Wallace, B. (2016); Checkoway, S., Cohney, S., Garman, C.; Green, M.; Heninger, N., Maskiewicz, J., Rescorla, E., Shacham, H., Weinmann, R.-P. (2016); Kim, P. (2016).

[77] McMillan, R. (2014): Verizon's "Perma-Cookie" is a Privacy-Killing Machine. In: WIRED, erschienen am: 27.10.2014, https://www.wired.com/2014/10/verizons-perma-cookie/ (06.03.2017).

[78] Aircrack-ng http://www.aircrack-ng.org/

[79] Github https://github.com/OpenSecurityResearch/hostapd-wpe

[80] Felt, A. P., Ainslie, A., Reeder, R. W., Consolvo, S., Thyagaraja, S., Bettes, A., Harris, H., und Grimes, J. (2015): Improving SSL warnings – Comprehension and adherence. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. ACM, New York, NY, USA, S. 2893-2902.

[81] Wie z. B. OpenWRT: https://openwrt.org

[82] Darunter: hostapd http://w1.fi/hostapd/; MadWifi http://madwifi-project.org/; aircrack-ng https://www.aircrack-ng.org; Karma http://digi.ninja/karma.

[83] Levine, B. (2015): RetailNext scores a whopping $125M to turn stores into data systems. Online: http://venturebeat.com/2015/04/15/retailnext-scores-a-whopping-125m-to-turn-stores-into-data-systems/ (01.12.2016).

[84] Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015): Unlocking the Potential of the Internet of Things. In: McKinsey Global Institute, erschienen im Juni 2015, http://goo.gl/qzq5mV (01.12.2016).

[85] Datoo, S. (2014): How tracking customers in-store will soon be the norm. In: The Guardian, erschienen am: 10.01.2014,

https://www.theguardian.com/technology/datablog/2014/jan/10/how-tracking-customers-in-store-will-soon-be-the-norm (01.12.2016); Gopalaratnam, S. (2015).

[86] Vgl. Gassen, M. and Fhom, H.S. (2016).

[87] Osborne, Charlie (2016): Transport for London to track commuters through Wi-Fi. In: Zdnet.com, erschienen am: 21.11.2016, http://www.zdnet.com/article/transport-for-london-to-track-commuters-through-wi-fi/ (08.03.2017); Robota, D. (2015): Ab sofort: Gratis-WLAN im Frankfurter Stadtgebiet. Online: https://www.op-online.de/region/frankfurt/gratis-wlan-frankfurter-stadtgebiet-freigeschaltet-alle-infos-5308218.html (08.03.2017).

[88] Bundesnetzagentur (o. J.): WLAN-Überwachung. Online: http://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/WLanUeberwachung/WLanUeberwachung_node.html (01.12.2016).

[89] Biselli, Anna (2015): Bundesnetzagentur will Überwachungseinrichtungen jetzt auch für WLAN-Hotspots. In: Netzpolitik.org, erschienen am: 24.02.2015, https://netzpolitik.org/2015/bundesnetzagentur-will-ueberwachungseinrichtungen-jetzt-auch-fuer-wlan-hotspots/ (01.12.2016).

[90] Lischka, K. (2013).

[91] Karaboga, M., Matzner, T., Mothes, C., Nebel, M., Ochs, C., Schütz, P., Fhom, H. S. (2014): „White Paper Selbstdatenschutz". In: Peter Zoche u. a. Hrsg.: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, 2. Aufl., Karlsruhe: Fraunhofer ISI. Online: https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Selbstdatenschutz_2.Auflage.pdf (25.2.2015).

[92] U.S. District Court (2014): „In the matter of a warrant to search a certain e-mail account controlled and maintained by Microsoft Corporation", U.S. District Court. Southern District of New York. Judge James C. Francis, 13 Mag. 2814, http://www.nysd.uscourts.gov/cases/show.php?db=special&id=398 (22.4.2015); Gibbs, Samuel (2014): US court forces Microsoft to hand over personal data from Irish server. In: The Guardian, erschienen am: 29.04.2014, http://www.theguardian.com/technology/2014/apr/29/us-court-microsoft-personal-data-emails-irish-server (22.4.2015).

[93] Vgl. z. B. Datoo (2014).

[94] Cohan, P. (2013): How Nordstrom Uses WiFi To Spy On Shoppers. In: forbes.com, erschienen am: 09.05.2013, http://www.forbes.com/sites/petercohan/2013/05/09/how-nordstrom-and-home-depot-use-wifi-to-spy-on-shoppers/#4d84f7153bf9 (01.12.2016); Gopalaratnam, S. (2015).

[95] Osborne, C. (2016); Hege, Hans (2016): Aufbau öffentlicher WLAN-Netze – Berliner Erfahrungen und Perspektiven. In: Netzpolitik.org, erschienen am: 10.06.2016, https://netzpolitik.org/2016/aufbau-oeffentlicher-wlan-netze-berliner-erfahrungen-und-perspektiven (08.03.2017); Hardy, Quentin (2013): Technology turns to tracking people offline. In: New York Times, erschienen am: 07.03.2013, http://bits.blogs.nytimes.com/2013/03/07/technology-turns-to-tracking-people-offline (08.03.2017); privacySIG (2015): Privacy in WiFi analytics. In: privacysig.org, erschienen am: 7.12.2015, http://www.privacysig.org/uploads/3/0/1/4/30147215/privacyinwifianalytics.pdf (01.12.2016).

[96] Datoo, S. (2014).

[97] Troianovski, A. (2012): New Wi-Fi Pitch: Tracker. In: The Wall Street Journal, erschienen am: 18.06.2012,

http://www.wsj.com/articles/SB10001424052702303379204577474961075248008 (01.12.2016).

[98] Angwin, J., & Tigas, M. (2015): Zombie Cookie: The Tracking Cookie That You Can't Kill. In: propublica.org, erschienen am: 14.01.2015, https://www.propublica.org/article/zombie-cookie-the-tracking-cookie-that-you-cant-kill (01.12.2016); Brodkin, J. (2015): AT&T's plan to watch your Web browsing – and what you can do about it. In: arstechnica.com, erschienen am: 27.03.2015, http://arstechnica.com/information-technology/2015/03/atts-plan-to-watch-your-web-browsing-and-what-you-can-do-about-it/3/ (01.12.2016).

[99] Datoo, S. (2014).

[100] Vanhoef, M., Matte, C., Cunche, M., Cardoso, L.S. and Piessens, F., (2016): Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM. S. 413-424; Datoo, S. (2014).

[101] Perez, Sarah (2013): RetailNext Acquires Eric Schmidt-Backed Wi-Fi Analytics Company, Nearbuy Systems. Online: https://techcrunch.com/2013/12/03/retailnext-acquires-eric-schmidt-backed-wi-fi-analytics-company-nearbuy-systems/ (01.12.2016).; Gopalaratnam, S. (2015).

[102] Datoo, S. (2014). Gopalaratnam, S. (2015).

[103] Vgl. Simo, Hervais/Gassen, Marius (2016).

[104] Für das Internet der Dinge vgl.: Karaboga, Murat, Tobias Matzner, Maxi Nebel, Carsten Ochs, Philip Schütz, Hervais Simo Fhom, Tina Morlok, Fabian Pittroff, Thilo von Pape, und Julia Victoria Pörschke (2015): White Paper Das versteckte Internet: Zu Hause - Im Auto - Am Körper. 1. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Karlsruhe: Fraunhofer-Institut für System- und Innovationsforschung. Online: https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Selbstdatenschutz_2.Auflage.pdf.
Zur Mobilfunkkomunikation vgl.: Spensky, C., Stewart, J., Yerukhimovich, A., Shay, R., Trachtenberg, A., Housley, R., & Cunningham, R. K. (2016): SoK: Privacy on Mobile Devices–It's Complicated. In: Proceedings on Privacy Enhancing Technologies, 2016 (3), 96-116; Park, Y. J., & Jang, S. M. (2014): Understanding privacy knowledge and skill in mobile communication. Computers in Human Behavior, 38, 296-303.

[105] IDC (2012): connected how smartphones and social keep us engaged. IDC Research Report; Bonné, Bram, Quax, Peter, Lamotte, Wim: Your Mobile Phone is a Traitor!–Raising Awareness on Ubiquitous Privacy Issues with SASQUATCH. In: International journal on information technologies & security. 6 (3), 2014.

[106] Martin, A. (2013a): Nordstrom Using Smart Phones To Track Customers Movements, erschienen am: 07.05.2013, http://dfw.cbslocal.com/2013/05/07/nordstrom-using-smart-phones-to-track-customers-movements/ (08.03.2017); Martin, A. (2013b): Nordstrom No Longer Tracking Customer Phones, erschienen am: 09.05.2013, http://dfw.cbslocal.com/2013/05/09/nordstrom-no-longer-tracking-customer-smart-phones/ (08.03.2017).

[107] Krowdthink (2016): Krowdthink Location Tracking & Data Report, S.19. Online: https://optmeoutoflocation.com/report.pdf (01.12.2016).

[108] Lischka, K. (2013).

[109] Levine, B. (2015).

[110] Clifford, S., and Hardy, Q. (2013): Attention, shoppers: Store is tracking your cell. In: NYT, erschienen am: 14.07.2013,

http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html (08.03.2017).

[111] Federal Trade Commission (2015): Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices. Online: https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers (1.12.2016); Cunche, M., Kaafar, M. A., and R. Boreli (2012), S. 1 (9).

[112] Krowdthink (2016), S.17; Die Deanonymisierung von Geolokationsdaten ist zudem besonders einfach: http://www.nature.com/articles/srep01376

[113] Xin, T., Guo, B., Wang, Z., Li, M. and Yu, Z. (2016): FreeSense: Indoor Human Identification with WiFi Signals. In: arXiv.org, arXiv preprint arXiv:1608.03430, erschienen am: 11.08.2016, http://arxiv.org/abs/1608.03430 (13.03.2017).

[114] Ali, K., Liu, A.X., Wang, W. and Shahzad, M. (2015): Keystroke recognition using wifi signals. In: Proceedings of the 21st Annual International Conference on Mobile Computing and Networking. ACM. S. 90-102. Online: http://dl.acm.org/citation.cfm?id=2790109 (08.03.2017).

[115] Wang, G., Zou, Y., Zhou, Z., Wu, K. and Ni, L. M. (2014): We can hear you with wi-fi! In: Proceedings of the 20th annual international conference on Mobile computing and networking. ACM. S. 593-604.

[116] Censky, A. (2011): Malls track shoppers' cell phones on Black Friday. In: CNNMoney, erschienen am: 22.11.2011, http://money.cnn.com/2011/11/22/technology/malls_track_cell_phones_black_friday/ (01.03.2017); Ein Zusammenschluss von einigen US-amerikanischen Unternehmen bietet zudem eine dauerhafte Opt-Out-Möglichkeit an, indem die WLAN MAC-Adresse und Bluetooth-Adresse in eine Opt-Out-Liste eingetragen wird, vgl.: https://smart-places.org/

[117] Schwan, Ben (2012): Freies Netz und Störerhaftung: „Es herrscht ein Durcheinander". In: Die Tageszeitung (taz), Abschn. Netzpolitik, erschienen am: 14.06.2012, http://www.taz.de/!5091507/ (17.11.2016).

[118] Bitkom (2013): Betreiber von WLAN-Hot-Spots brauchen Rechtssicherheit. In: bitcom.org, erschienen am: 06.06.2013, https://www.bitkom.org/Presse/Presseinformation/Betreiber-von-WLAN-Hot-Spots-brauchen-Rechtssicherheit.html (27.07.2016).

[119] Forum der Rechteinhaber (2007): Das Forum der Rechteinhaber nimmt Stellung zu den Fragen zur Regelung der Anbieterhaftung im Telemediengesetz (TMG) des Bundesministeriums für Wirtschaft und Technologie, erschienen am: 31.08.2007, http://www.musikindustrie.de/fileadmin/piclib/politik/nationale_ggvorhaben/pp_gesetz_nat_stellungn_20070831_forum_tmg.pdf (27.07.2016).

[120] Hawiger, Daniel (2015): Die Abmahnindustrie – Wie deutsche Rechtsanwälte gegen EU-Recht verstoßen. In: Netzpolitik.org, erschienen am: 08.07.2015, https://netzpolitik.org/2015/die-abmahnindustrie-wie-deutsche-rechtsaenwaelte-gegen-eu-recht-verstossen/ (28.07.2016).

[121] CDU, CSU und SPD (2013): Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD. 18. Legislaturperiode, S. 48 f. Online: http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf?__blob=publicationFile (25.07.2016).

[122] BMWi, BMI, and BMVI (2014): Digitale Agenda 2014 – 2017. Berlin, S.15. Online: http://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda.pdf?__blob=publicationFile&v=6 (25.07.2016).

[123] Digitale Gesellschaft e. V. (o. J.): WLAN-Störerhaftung beseitigen. Online: https://digitalegesellschaft.de/mitmachen/storerhaftung-beseitigen/ (29.07.2016).

[124] Sawall, Achim (2014): Gesetz gegen Störerhaftung von WLANs im August. In: Golem.de, erschienen am: 02.07.2014, http://www.golem.de/news/bundeswirtschaftsminister-gesetz-gegen-stoererhaftung-von-wlans-im-august-1407-107594.html (27.07.2016).

[125] Dörner (2016).

[126] Heise, C. (2015): Böses Netz. In: Süddeutsche Zeitung, erschienen am: 23.04.2015, http://www.sueddeutsche.de/digital/aussenansicht-boeses-netz-1.2447111 (08.03.2017).

[127] BT-Drs 18/3047 (2014): Entwurf eines Gesetzes zur Änderung des Telemediengesetzes – Störerhaftung, Gesetzentwurf der Fraktion Bündnis 90/Die Grünen und der Fraktion Die Linke vom 05.11.2014. Online: http://dip21.bundestag.de/dip21/btd/18/030/1803047.pdf (28.03.2017). Vgl. auch: Digitale Gesellschaft e. V. (2012): Entwurf eines Gesetzes zur Änderung des Telemediengesetzes. Online: https://digitalegesellschaft.de/wp-content/uploads/2012/06/Digitale-Gesellschaft-Gesetzentwurf-Haftungsfreistellung-fur-offentliche-Funknetzwerke.pdf (27.07.2016).

[128] Deutscher Bundestag (2016): Bundestagsbeschlüsse am 2. und 3. Juni, vom 03.06.2016. Online: https://www.bundestag.de/dokumente/textarchiv/2016/kw22-angenommen-abgelehnt/425518 (27.07.2016).

[129] Beschlussempfehlung und Bericht des Ausschusses für Wirtschaft und Energie (2015): Entwurf eines Gesetzes zur Änderung des Telemediengesetzes – Störerhaftung, Drs. 18/3861 vom 28.01.2015. Online: http://dip21.bundestag.de/dip21/btd/18/038/1803861.pdf (27.07.2016).

[130] Referentenentwurf (2015): Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMÄndeG), vom 17.02.2015. Online: https://netzpolitik.org/wp-upload/2015-02-17_Referentenentwurf-Telemedien%C3%A4nderungsgesetz.pdf (27.07.2016).

[131] Abgestimmter Referentenentwurf (2015): Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMÄndeG), vom 11.03.2015. Online: http://www.bmwi.de/BMWi/Redaktion/PDF/S-T/telemedienaenderungsgesetz,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (28.03.2017).

[132] Forum der Rechteinhaber (2015a): Stellungnahme des „Forum der Rechteinhaber" zur Anpassung der Haftungsprivilegien. Erschienen am: 8.04.2015, https://www.vg-media.de/images/stories/pdfs/stellungnahmen/stellungnahme_referentenentwurf_tmg.pdf (27.07.2016).

[133] Digitale Gesellschaft (2015): FAQ zur WLAN-Störerhaftung: Sie können es nicht. Online: https://digitalegesellschaft.de/2015/04/stoererhaftung-sie-koennen-es-nicht/ (08.03.2017); Verbraucherzentrale Bundesverband (vzbv) (2015): Haftungsbefreiung für WLAN stärken, erschienen am: 7.04.2015, https://www.bmwi.de/BMWi/Redaktion/PDF/Stellungnahmen/Stellungnahmen-WLAN/verbraucherzentrale-bund,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (29.07.2016).

[134] ECO (2015): Stellungnahme zum Referentenentwurf eines Zweiten Gesetzes zur Änderung des TMG, 1. Erschienen am: 09.04.2015, https://www.eco.de/wp-content/blogs.dir/20150408-eco-stellungnahme-2.telemedienaendg.pdf vom 09.04.2015. (28.07.2016).

[135] Beckedahl, Markus (2015): EU-Kommission kritisiert Gesetz-Entwurf zur Verschlimmbesserung der Störerhaftung. In: Netzpolitik.org, erschienen am: 03.12.2015,

Anmerkungen

https://netzpolitik.org/2015/eu-kommission-kritisiert-gesetz-entwurf-zur-verschlimmbesserung-der-stoererhaftung/ (27.07.2016).

[136] Digitale Gesellschaft e. V., Förderverein Freie Netzwerke e. V. und Verbraucherzentrale Bundesverband e. V. (vzbv) (2015): Notifizierungsnummer: 2015/0305/D - SERV60, erschienen am: 6. Juli 2015, https://digitalegesellschaft.de/wp-content/uploads/2015/07/Notifizierung2015-0305-D.pdf (27.07.2016).

[137] Bundesrat (2015): Stellungnahme des Bundesrates. Entwurf eines Zweiten Gesetzes zur Änderungen des Telemediengesetzes. Online: https://www.bundesrat.de/SharedDocs/drucksachen/2015/0401-0500/440-15%28B%29.pdf?__blob=publicationFile&v=1 (28.07.2016).

[138] Dazu https://www.bundestag.de/dokumente/textarchiv/2015/kw51-pa-wirtschaft/398718 und auch: https://digitalegesellschaft.de/2015/12/anhoerung-tmg-wie-weiter/; Siehe auch: Forum der Rechteinhaber (2015b): Stellungnahme des „Forum der Rechteinhaber" zur Anpassung der Haftungsprivilegien. 04.12.2015. Online: https://netzpolitik.org//wp-upload/haftungsprivileg_forum_rechteinhaber.pdf (27.07.2016).

[139] EuGH, Urteil v. 15. 9. 2016, Rs.C-484/14.

[140] Briegleb, V. (2016), Keine Störerhaftung bei öffentlichen WLANs: Bundesrat winkt Gesetzesänderung durch. In: heise online, erschienen am: 17.06. 2016, http://www.heise.de/newsticker/meldung/Keine-Stoererhaftung-bei-oeffentlichen-WLANs-Bundesrat-winkt-Gesetzesaenderung-durch-3240704.html (29.1.2016); BMWI (2016): Mehr Rechtssicherheit bei WLAN. Online: http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan.html (29.11.2016).

[141] Gesetz vom 21.7.2016, BGBl. I, S. 1766.

[142] BT-Drs. B 18/8645 v. 1.6.2016, S. 7.

[143] Siehe dazu z. B. Franz, T., Sakowski, P. (2016): Die Haftung des WLAN-Betreibers nach der TMG-Novelle und den Schlussanträgen des Generalanwalts beim EuGH. In: CR - Computer und Recht, Heft 8, S. 527; Reinbold, F. (2016), Ende der Störerhaftung. In: Spiegel online, erschienen am: 31.5.2016, http://www.spiegel.de/netzwelt/netzpolitik/stoererhaftung-so-will-der-bundestag-das-wlan-freier-machen-a-1095125.html (13.03.2017); Beuth, P. (2016), Der Totenschein der Störerhaftung. In: Die Zeit, erschienen am: 31.5.2016, http://www.zeit.de/digital/internet/2016-05/wlan-hotspots-stoererhaftung-abmahnungen-unterlassung (29.11.2016).

[144] Spindler, G. (2016), Die neue Providerhaftung für WLANs – Deutsche Störerhaftung adé? In: Neue Juristische Woche (NJW), Heft 34, S. 2449.

[145] EuGH, Urteil v. 15. 9. 2016.

[146] BGH, Urt. v. 11.03.2004, Rs. I ZR 304/01, BGH, Urt. v. 17.5.2001, Rs. I ZR 251/99; Jandt, S. (2013), in: Roßnagel, A. (Hrsg.), Recht der Telemediendienste, § 7 TMG, Rn. 49; Hoeren, T., n: Hoeren, T.,Sieber, U.,Holznagel, B., Recht der elektronischen Medien, Teil 18, Rn. 70.

[147] Mantz, R., Sassenberg, T. (2014a), S. 3541; Ufer, F. (2007), Die Haftung der Internet Provider nach dem Telemediengesetz. Hamburg: Verlag Dr. Kovač. S. 134.

[148] Ausführlich zur Störerhaftung s. z. B. Volkmann, C. (2005): Die Störerhaftung im Internet , S. 56 ff.

[149] Jandt (2013); Mantz, R., Sassenberg, T. (2014b): WLAN und Recht: Aufbau und Betrieb von Internet-Hotspots. Erich Schmidt Verlag, S. 160; Borges, G. (2010), Pflich-

ten und Haftung beim Betrieb privater WLAN. In: Neue Juristische Woche (**NJW**), S.2624; Mantz, R., Sassenberg, T. (2014a), S. 3540.

[150] Dazu ausführlich z. B. Hoffmann, H. (2015), in: Spindler, G.,Schuster, F. (Hrsg.), Recht der elektronischen Medien, 12. Teil, § 8 TMG, Rn. 20-25.

[151] Mantz, R., Sassenberg, T. (2014a), S. 3540; Bär, W. (2014), in: Wabnitz, H.-B.,Janowsky, T. (Hrsg.), Handbuch des Wirtschafts- und Steuerfachrechts, 14. Kapitel, Rn. 189.

[152] Hullen, N. (2015): Referentenentwurf zur Lockerung der Störerhaftung für Betreiber öffentlicher WLANs. In: jurisPR-ITR, 7/2015, Anm. 2; Digitale Gesellschaft e. V. (o. J.).

[153] Lutz, S. (2010): Verteidigungsstategien bei Filesharing-Abmahnungen. In: Verbraucher und Recht (VuR), Heft 9, S. 337-345 (342); Mantz, R., Sassenberg, T. (2014a); Hullen, N. (2015); Digitale Gesellschaft e. V. (o. J.).

[154] S. z. B. AG Hamburg, Urteil v. 10.06.2014, Rs. 25b C 431/13; OLG Frankfurt v. 18.07.2014, Rs. 6 U 192/1; MMR 2014, 625; Hoeren, T., Jakopp, S. (2014): WLAN-Haftung – A never ending story? In: Zeitschrift für Rechtspolitik (ZRP) 47, Nr. 3, S. 72; Mantz, R.,Sassenberg, T. (2014a) S. 3541.

[155] Digitale Gesellschaft e. V. (o. J.).

[156] Mantz, R., Sassenberg, T. (2014a).

[157] BGH, Urteil v. 12.05.2010, Rs. I ZR 121/08.

[158] Filesharing bezeichnet (vereinfacht ausgedrückt) den unberechtigten Austausch von Werken im Internet, die urheberrechtlich geschützt sind, mittels einer Client-Software. Mit Hilfe dieser Computerprogramme ermöglichen die Inhaber virtueller Tauschbörsen ihren Mitgliedern einen uneingeschränkten und kostenlosen Zugriff auf alle die im Netz vorhandenen Daten zum Zeitpunkt der jeweiligen Internetverbindung; s. dazu Popescu, P. (2011): Verschuldensunabhängige Störerhaftung für den unzureichend gesicherten WLAN-Anschluss. In: Verbraucher und Recht (VuR) S. 327.

[159] Conraths, T., Peintinger, S. (2016): Der neue § 8 TMG: Kein Wegfall der Störerhaftung von W-LAN-Betreibern. In: GRUR-Prax 2016, Nr. 14, S. 297.

[160] Ausführlich zur Störerhaftung im BGH-Urteil „Sommer unseres Lebens“ s. z. B. Popescu, P. (2011), Borges, G. (2010).

[161] Jandt, S. (2013), Rn. 4.

[162] § 7 Abs. 2 Satz 2 TMG; Umsetzung ins nationale Recht durch Art. 12 Abs. 3, Art 13 Abs. 2 und Art. 14 Abs. 3 der E-Commerce-Richtlinie.

[163] Jandt, S. (2013), Rn. 46; Mantz, R., Sassenberg, T. (2014b), S. 155.

[164] Zu den Schlussanträgen des Generalanwalts Maciej Szpunar vom 16.3.2016 in der Rechtssache McFadden/Sony Music, http://curia.europa.eu/juris/document/document.jsf?docid=175130&doclang=de (29.11.2016).

[165] EuGH, Urteil v. 15. 9. 2016, Rn. 41 bis 43.

[166] EuGH, Urteil v. 15. 9. 2016, Rn. 55 ff.

[167] EuGH, Urteil v. 15. 9. 2016, Rn. 67.

[168] EuGH, Urteil v. 15. 9. 2016, Rn. 71.

[169] EuGH, Urteil v. 15. 9. 2016, Rn. 76 bis 78.

[170] EuGH, Urteil v. 15. 9. 2016, Rn. 87.

[171] EuGH, Urteil v. 15. 9. 2016, Rn. 88 und 89.

Anmerkungen

[172] EuGH, Urteil v. 15. 9. 2016, Rn. 90 ff.

[173] EuGH, Urteil v. 15. 9. 2016, Rn. 90 und 101.

[174] Szpunar, Schlussanträge v. 16.3.2016, Rn. 137 bis 143; dazu ausführlich Franz, T., Sakowski, P. (2016), S. 524, 529 f.; EuGH, Urteil v. 15. 9. 2016, Rn. 10; Szpunar, Schlussanträge v. 16.3.2016, Rn. 147.

[175] Diese wird als zivilrechtliche verschuldensunabhängige Haftung angesehen.

[176] BT-Drs. B 18/8645 v. 1. 6. 2016, S. 10; Szpunar, Schlussanträge v. 16.3.2016, Rn. 115 und 151.

[177] BT-Drs. B 18/8645 v. 1. 6. 2016, S. 10; siehe dazu ausführlich Franz, T., Sakowski, P. (2016), S. 529 f.

[178] Szpunar, Schlussanträge v. 16.3.2016, Rn. 137 bis 143.

[179] Assion, S. (2016): 5 Fragen zum WLAN-Urteil des EuGH, Punkt 3. In: Telemedicus, erschienen am: 23. 9. 2016, http://tlmd.in/a/3130 (29.11.2016).

[180] Mantz, R. (2016a), WLAN-Störerhaftung, Punkt 8b. In: Telemedicus, erschienen am: 17. 3. 2016, http://tlmd.in/a/3068 (27.11.2016); zur Unterscheidung zwischen privaten und gewerblichen Anbietern s. ausführlich Mantz, R., /Sassenberg, T. (2016b): Betrieb eines öffentlichen WLANs – Der unbeschränkte Internetzugang als „Vertragsinhalt?. In: Computer und Recht (CR), S. 298.

[181] Eine Unterscheidung zwischen den Diensteanbietern hätte einen Bruch in der Systematik des TMG bedeutet. Um dies zu vermeiden und da das Unionsrecht einer abweichenden Regelung nicht entgegensteht, hat sich die deutsche Gesetzgebung für diese weitreichende Lösung entschieden; siehe dazu Spindler, G. (2016), S. 2450.

[182] Dazu z. B. Kischel, U. (2016), in: Epping, V., Hillgruber, C. (Hrsg.), Grundgesetz Kommentar, Art. 3 GG, Rn. 1 ff.

[183] Assion, S. (2016); A. A. Buermeyer; er vertritt die Ansicht, dass weder der EuGH noch das Unionsrecht verlangen, dass das nationale Recht überhaupt gerichtliche oder behördliche Verfügungen gegen WLAN-Anbieter vorsehen muss; Buermeyer, U. (2016): Analyse des EuGH-Urteils zur Störerhaftung. In: heise online, erschienen am: 15.09.2016, https://heise.de/-3324825 (27.11.2016).

[184] BGH, Urteil v. 11. 3. 2004, Rs.I ZR 304/01.

[185] Art. 12 Abs. 3, 13 Abs. 2 und 14 Abs. 3; E-Commerce-RL lassen diese Vorschriften ebenfalls unberührt, sodass ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten von den Diensteanbietern verlangen kann, die Rechtsverletzung abzustellen oder zu verhindern.

[186] EuGH, Urteil v. 27. 3. 2014, Rs. C-314/12.

[187] Härting, N. (2016): Warum die Kritik an den neuen WLAN-Vorschlägen fehl geht. In: CRonline, erschienen am: 1. 6. 2016, http://www.cr-online.de/blog/2016/06/01/warum-die-kritik-an-den-neuen-wlan-vorschlaegen-fehl-geht/ (27.11.2016).

[188] EuGH, Urteil v. 15. 9. 2016, Rn. 83 ff.

[189] Nach der Rechtsprechung des EuGH umfasst der Begriff „Vermittler" auch die Access Provider; EuGH, Urteil v. 19. 2. 2009, Rs.C-557/07, Rn. 324

[190] EuGH, Urteil v. 15. 9. 2016.

[191] BGH, Urteil v. 26. 11. 2015, Rs. I ZR 174/14.

Anmerkungen

[192] Dies sehen auch die europarechtlichen Vorgaben zum Schutz der Urheber und sonstiger Rechteinhaber in Art. 8 Abs. 3 E-Commerce-RL und Art. 11 S. 3 Durchsetzungs-RL vor, von denen die deutsche Gesetzgebung nicht ohne weiteres abweichen kann.

[193] EuGH, Urteil v. 19. 2. 2009, Rn. 96 bis 101.

[194] EuGH , Urteil v. 19. 2. 2009, Rn. 81.

[195] EuGH, Urteil v. 19. 2. 2009, Rn. 96.

[196] Siehe dazu Piltz, C. (2016): Datenschutzrechtliche Folgen des EuGH-Urteil. In: De Lege Data, erschienen am: 15. 9. 2016, https://www.delegedata.de/2016/09/datenschutzrechtliche-folgen-des-wlan-urteils-des-eugh/ (27.11.2016).

[197] Assion, S. (2016).

[198] EuGH, Urteil v. 15. 9. 2016, Rn. 78.

[199] Ausführlich zur Strafbarkeit des Angreifers auf WLAN-Netzwerke Nebel, ZD-aktuell 2016, 05323.

[200] Graf, in: MüKo 2012, § 202b StGB, Rn. 10.

[201] Mit Verweis auf das WLAN-Scanning bei Google Street View Gercke, ZUM 2010, 633 (644); ders., in: Spindler/Schuster 2015, § 202b StGB, Rn. 5.

[202] Dazu z. B. Fischer 2016, § 263a StGB, Rn. 22.

[203] Zum untauglichen Versuch z. B. Fischer 2016, § 22 StGB, Rn. 39 ff.

[204] Stree/Hecker, in: Schönke/Schröder 2014, § 303a StGB, Rn. 1; Weidemann, in: v. Heintschel-Heinegg 2016, § 303a StGB, Rn. 2; Fischer 2016, § 303a StGB, Rn. 2.

[205] So Fischer 2016, § 303a StGB, Rn. 3.

[206] Unberechtigtes Kopieren von Daten ist nicht vom Tatbestand des § 303 StGB umfasst, Weidemann, in: v. Heintschel-Heinegg 2016, § 303a StGB, Rn. 13.

[207] S. dazu Abschnitt 4.3.3.

[208] Fischer 2016, § 303b StGB, Rn. 12; Wieck-Noodt, in: MüKo 2014, § 303b StGB, Rn. 12.

[209] Wieck-Noodt, in: MüKo 2014, § 303b StGB, Rn. 23 mit weiteren Nachweisen.

[210] Fischer 2016, § 303b StGB, Rn. 9.

[211] Stree/Hecker, in: Schönke/Schröder 2014, § 303b StGB, Rn. 9.

[212] Sternberg-Lieben/Hecker, in: Schönke/Schröder 2014, § 317 StGB, Rn. 2.

[213] Sternberg-Lieben/Hecker, in: Schönke/Schröder 2014, § 317 StGB, Rn. 3 mit Verweis auf § 316b StGB, Rn. 7.

[214] Altenhain, in: MüKo-StGB, § 148 TKG, Rn. 16.

[215] Altenhain, in: MüKo-StGB, § 148 TKG, Rn. 17.

[216] Mantz, R., Sassenberg, T. 2014a, S. 3537, 3539.

[217] Spindler, Gerald; Schuster, Fabian; Döpkens, Harm-Randolf (Hg.) (2015): Recht der elektronischen Medien. Kommentar. 3. Aufl. München: Beck, TKG § 88, Rn. 26.

[218] Bock, in: Beck'scher TKG Kommentar, 4. Aufl. 2013, § 88 TKG, Rn 24; Spindler, G., Schuster, F., Döpkens, H.-R. (2015), TKG § 88, Rn. 28; a.A.: LAG Berlin-Brandenburg, Urteil v. 16.02.2011, Az.: 4 Sa 2132/10.

Anmerkungen

[219] Bock, M. (2013): §§88-90. In: Geppert, M., Schütz, R., Attendorn, T. (Hrsg.), Beck'scher TKG Kommentar. 4. Aufl. München: Beck, § 88 TKG, Rn 1; Spindler, G., Schuster, F., Döpkens, H.-R. (2015), TKG § 88 Rn. 2.

[220] Durner, in: Maunz/Dürig/Durner, Grundgesetz-Kommentar, 77. EGL 2016, Rn 43.

[221] Siehe Abschnitt 3.2.

[222] Bock, in: Geppert/Schütz (Hrsg.), Beck'scher TKG Kommentar, 4. Aufl. 2013, § 88 TKG, Rn 26.

[223] Braun, in: Geppert/Schütz (Hrsg.), Beck'scher TKG Kommentar, 4. Aufl. 2013, § 91 TKG, Rn 15 ff.

[224] Braun, in: Geppert/Schütz (Hrsg.), Beck'scher TKG Kommentar, 4. Aufl. 2013, § 91 TKG, Rn 8.

[225] Büttgen, in: Geppert/Schütz (Hrsg.), Beck'scher TKG Kommentar, 4. Aufl. 2013, § 95 TKG, Rn 3 ff.

[226] Braun, in: Geppert/Schütz (Hrsg.), Beck'scher TKG Kommentar, 4. Aufl. 2013, § 3 TKG, Rn 93.

[227] EuGH, Urteil v. 15. 9. 2016, Rn. 96 ff.

[228] Reber, in: Ahlberg/Götting, Beck'scher TKG-Kommentar Urheberrecht, 14. Edition, Stand 01.10.2016, § 102 UrhG, Rn 2.

[229] EuGH, Urteil v. 19. 10. 2016, Az.: C-582/14.

[230] Büttgen, in: Beck'scher TKG-Kommentar, 4. Aufl. 2013, § 95 Rn. 28.

[231] Braun, in: Geppert/Schütz (Hrsg.), Beck'scher TKG-Kommentar, 4. Aufl. 2013, § 96 TKG Rn. 22.

[232] Bock, in: Geppert/Schütz (Hrsg.), Beck'scher TKG Kommentar, 4. Aufl. 2013, § 88 TKG, Rn 28 ff.

[233] Bock, in: Geppert/Schütz (Hrsg.), Beck'scher TKG Kommentar, 4. Aufl. 2013, § 88 TKG, Rn 49, 50.

[234] Mitteilung der Bundesnetzagentur zur Meldepflicht nach § 6 Telekommunikatonsgesetz (TKG) (Nr. 149/2015); kritisch hierzu Sassenberg/Mantz (2015): Die Meldepflicht nach § 6 TKG – Mitteilung Nr. 149/2015 der Bundesnetzagentur und ihre Folgen. In: Multimedia und Recht (MMR) 2015, Nr. 7, S. 428ff.

[235] BT-Drs. 18/5088 vom 09.06.2015, S. 37

[236] Vgl. Simo/Gassen (2016).

[237] Emmerich, in: Münchener Kommentar zum BGB, 7. Aufl. 2016, § 311, Rn 46.

[238] Wolff, in Beck'scher Online-Kommentar Datenschutzrecht, 17. Edition 2015, § 28 Rn. 33.

[239] Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, 4. Aufl. 2014, § 28 Rn. 57; Wolff, in: Beck'scher Online-Kommentar Datenschutzrecht,

[240] BVerfG, NJW 1970, 235, 237; Wolff, in: Beck'scher Online-Kommentar Datenschutzrecht, 17. Edition 2015,§ 28 Rn. 80; Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, 4. Aufl. 2014, § 28 Rn. 58.

[241] Wolff, in: Beck'scher Online-Kommentar Datenschutzrecht, 17. Edition 2015,§ 28 Rn. 81.1; Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, 4. Aufl. 2014, § 28 Rn. 58.

[242] BGH, NJW 2013, 2530, 2533.

[243] Simitis, in: Simits, BDSG, 8. Aufl. 2014,§ 4a Rn.27.

[244] Simitis, in: Simitis, BDSG, 8. Aufl. 2014, § 4a Rn. 44.

[245] Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 28 Rn. 31; Simitis, in: Simitis, BDSG, 8. Aufl. 2014, § 28 Rn. 163.

[246] Schantz, NJW, 2016, 1841, 1845.

[247] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10.01.2017, abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52017PC0010.

[248] In der Vergangenheit wurde allerdings gezeigt, dass Android Smartphones auch dann noch Probe Requests aussenden, wenn das WLAN deaktiviert wurde. Siehe: Wischnjak, D., Eikenberg, R. (2014): Auf Schritt und Tritt. Smartphones arbeiten unbemerkt als Peilsender. In: C'T, Heft 21, S. 158-161.

[249] bcrypt (http://bcrypt.sourceforge.net/)

[250] Future of Privacy Forum (2013): Mobile Location Analytics Code of Conduct, erschienen am: 22.10.2013, http://www.futureofprivacy.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf (28.03.2017).

[251] Zebra Technologies (2014): Analysis of iOS 8 MAC Randomization on Locationing. Whitepaper. Online: http://mpact.zebra.com/documents/iOS8-White-Paper.pdf (28.03.2017).

[252] AirTightTeam (2014): iOS8 MAC Address Randomization Update. Online: http://blog.mojonetworks.com/ios8-mac-randomgate/ (28.03.2017).

[253] Skinner, K. and Novak, J. (2015): Privacy and Your App. In: Worldwide Developers Conference (WWDC). Apple.

[254] Vanhoef, M., Matte, C., Cunche, M., Cardoso, L.S. and Piessens, F. (2016): Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, ACM, S. 413-424.

[255] Huitema, C., (2015): Experience with MAC address randomization in Windows 10. In: 93th Internet Engineering Task Force Meeting (IETF); Privacy Handbuch. MAC-Adresse faken für Windows 10. Online: https://www.privacy-handbuch.de/handbuch_27b.htm. (28.03.2017).

[256] Google Inc. (2015): Android 6.0 changes - Access to Hardware Identifier. Online: https://developer.android.com/about/versions/marshmallow/android-6.0-changes.html#behavior-hardware-id (01.03.2017).

[257] Copperhead (2016): Technical overview of CopperheadOS. Online: https://copperhead.co/android/docs/technical_overview (28.03.2017).

[258] Vanhoef, M., Matte, C., Cunche, M., Cardoso, L.S. and Piessens, F. (2016): Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM. S. 413-424.

[259] Fluhrer, S., Mantin, I., & Shamir, A. (2001): Weaknesses in the key scheduling algorithm of RC4. In: International Workshop on Selected Areas in Cryptography. Springer: Berlin Heidelberg. S. 1-24.

[260] Eckert, C. (2013): IT-Sicherheit: Konzepte-Verfahren-Protokolle. Walter de Gruyter.

[261] Wi-Fi Alliance: http://www.wi-fi.org

Anmerkungen

[262] Rigney, C., Willens, S., Rubens, A., Simpson, W. (2000): IETF. RFC 2865: Remote Authentication Dial In User Service (RADIUS). Online: http://www.rfc-editor.org/rfc/rfc2865.txt (17.03.2017).

[263] Dierks, T., Rescorla, E. (2008): The transport layer security (TLS) protocol version 1.2. Online: https://tools.ietf.org/html/rfc5246?as_url_id=AAAAAAXYO7GMXCsarKPwoGgdRmNPulmTyUCpaMS0WHll8s9nzhvgZQc67JucPlX3eSXPmfCgPvw52FpSceviDTaMSpBR (17.03.2017).

[264] Portswigger: https://portswigger.net/burp/proxy.html

[265] Moxie: https://moxie.org/software/sslstrip/

[266] Lanze, F., Panchenko, A., Ponce-Alcaide, I., and Engel, T. (2014): Undesired relatives: protection mechanisms against the evil twin attack in ieee 802.11. In: Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks, ACM, S. 87 (94).

[267] K. Heyman (2007): A new virtual private network for today's mobile world. In: Computer 40, Nr. 12, S. 17–19; Alshalan, A., Pisharody, S., & Huang, D. (2016): A Survey of Mobile VPN Technologies. In: IEEE Communications Surveys & Tutorials 18, Nr. 2, S. 1177-1196.

[268] Tzvetkov, V. D. (2010): Virtual private networks for mobile environments. Development of protocol for mobile security and algorithms for location update. Ph.D. dissertation, Tech. Dept. Comput. Sci., Tech. Univ. Darmstadt, Darmstadt, Germany.

[269] Perta, Vasile C., et al. (2015): A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients. In: Proceedings on Privacy Enhancing Technologies 2015.1, S. 77-91.

[270] Wired: How VPN use varies by country. Online: http://www.wired.co.uk/gallery/vpn-use-varies-by-country (17.03.2017).

[271] Perta, Vasile C., et al. (2015).

[272] AVM VPN Service-Portal: VPN-Verbindung zur FRITZ!Box unter Android einrichten. Online: https://avm.de/service/vpn/tipps-tricks/vpn-verbindung-zur-fritzbox-unter-android-einrichten/ (17.03.2017).

[273] Torproject (2016): Mehr als 2000 relays and bridges im Tor-Netzwerk. Online: https://metrics.torproject.org/networksize.html (31.10.2016)

[274] Karaboga, M., Masur, P., Matzner, T., Mothes, C., Nebel, M., Ochs, C., Schütz, P., Fhom, H. S. (2014): White Paper Selbstdatenschutz. 2. Aufl. Karlsruhe: Fraunhofer ISI (Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt). Online: https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Selbstdatenschutz_2.Auflage.pdf (17.03.2017).

[275] Beyah, R., & Venkataraman, A. (2011): Rogue-access-point detection: Challenges, solutions, and future directions. In: IEEE Security and Privacy 9, Nr. 5, S. 56-61; Gonzales, H., Bauer, K., Lindqvist, J., McCoy, D., & Sicker, D. (2010): Practical defenses for evil twin attacks in 802.11. In: Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. IEEE. S. 1-6.

[276] Mustafa, H., & Xu, W. (2014): CETAD: Detecting evil twin access point attacks in wireless hotspots. In: Communications and Network Security (CNS), 2014 IEEE Conference on. IEEE. S. 238-246; Nakhila, O., Dondyk, E., Amjad, M. F., & Zou, C. (2015): User-Side Wi-Fi Evil Twin Attack Detection Using SSL/TCP Protocols. In: 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC). IEEE. S. 239-244; Yang, C., Song, Y. and Gu, G. (2012): Active user-side evil twin access point

detection using statistical techniques. In: IEEE Transactions on Information Forensics and Security 7, Nr. 5, S. 1638-1651; Song, Y., Yang, C. and Gu, G. (2010): Who is peeping at your passwords at Starbucks? – To catch an evil twin access point. In: Proceedings of the 2010 IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 10, S. 323-332.

[277] Zheng, X., Wang, C., Chen, Y., & Yang, J. (2014): Accurate rogue access point localization leveraging fine-grained channel information. In: Communications and Network Security (CNS), 2014 IEEE Conference on. IEEE. S. 211-219.

[278] Arackaparambil, C., Bratus, S., Shubina, A., & Kotz, D. (2010): On the reliability of wireless fingerprinting using clock skews. In: Proceedings of the third ACM conference on Wireless network security. ACM. S. 169–174; Jana, S., & Kasera, S. K. (2010): On fast and accurate detection of unauthorized wireless access points using clock skews. In: Mobile Computing, IEEE Transactions on 9, Nr. 3, 449–462.

[279] Mustafa, H., & Xu, W. (2014).

[280] Lanze, F., Panchenko, A., Ponce-Alcaide, I., & Engel, T. (2015). Hacker's toolbox: Detecting software-based 802.11 evil twin access points. In: 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC). IEEE. S. 225-232.

[281] Gonzales, H., Bauer, K., Lindqvist, J., McCoy, D., & Sicker, D. (2010): Practical defenses for evil twin attacks in 802.11. In: Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, S. 1-6; Bauer, K., Gonzales, H., & McCoy, D. (2008). Mitigating evil twin attacks in 802.11. In: 2008 IEEE International Performance, Computing and Communications Conference. IEEE. S. 513-516.

[282] Steinhau, Henry (2013): Ben Scott: „Das Internet ist zu einem öffentlichen Gut geworden". In: irights.info, erschienen am: 10.09.2013, https://irights.info/artikel/ben-scott-das-internet-ist-zu-einem-offentlichen-gut-geworden/17632 (13.03.2017).

[283] A.A.K. (2013): How did Estonia become a leader in technology? In: economist.com, erschienen am: 31.07.2013, http://www.economist.com/blogs/economist-explains/2013/07/economist-explains-21 (13.03.2017).

[284] Fernholz, Tim (2014): Barack Obama says the internet is a public good, and that's why the US needs net neutrality. In: Quartz, erschienen am: 10.11.2014, http://qz.com/293904/barack-obama-says-the-internet-is-a-public-good-and-thats-why-the-us-needs-net-neutrality/ (17.03.2017).

[285] Erwähnenswert in diesem Zusammenhang ist die vergleichsweise neuartige Praxis der Minimierung der Haftungsrisiken, indem Geschäftsinhaber, die ein öffentliches WLAN anbieten wollen, nicht selber eins einrichten, sondern auf WLAN-Hotspot-Zugänge von Internet-Providern zurückgreifen, die sich um Betrieb, Konfiguration und Haftungsfragen kümmern. Dies erleichtert wiederum Geschäftsinhabern die Entscheidung, öffentliches WLAN anzubieten. Vgl. dazu: Mansmann, Urs (2016): Geteiltes Glück: WLAN für Kunden und Gäste. In: C't 2016, Nr. 22, S. 72-74.

Anhang

Abkürzungsverzeichnis

AP	Access point (Zugangspunkt)
AES	Advanced Encryption Standard
AGB	Allgemeine Geschäftsbedingungen
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BS	Basic service set
BSSID	Basic service set identifier
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DS	Distribution System
DSGVO	Datenschutz-Grundverordnung
EuGH	Europäischer Gerichtshof
ESS	Extended Service Set
GG	Grundgesetz
HTTP(S)	Hypertext Transfer Protocol (Secure); (sicheres) Hypertext-Übertragungsprotokoll
IBSS	Independent basic service set
IP	Internet Protokoll
ISP	Internet Service Provider
LAN	Local area network
MAC	*Media Access Control*
MIC	Message Integrity Check-
MITM	Man-in-the-middle (Mittelsmann-Angriff)
nPA	Neuer Personalausweis
PSK	Pre-shared key
SDP	Service Discovery Protocol
SSID	Service set identifier (Netzwerkname)
SSL	Secure Socket Layer
STA	Station
StGB	Strafgesetzbuch
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
VPN	Virtuelles privates Netzwerk
WDS	Wireless Distribution System (WLAN-Repeater)
WEP	Wired Equivalent Privacy
(W)LAN	(Wireless) Local Area Network (Lokales drahtloses Netzwerk bzw. lokales Funknetzwerk)

IMPRESSUM

Kontakt:
Michael Friedewald
Geschäftsfeldleiter „Informations- und Kommunikationstechnik“

Telefon +49 721 6809-146
Fax +49 721 6809-315
E-Mail info@forum-privatheit.de

Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

www.isi.fraunhofer.de
www.forum-privatheit.de

Schriftenreihe:
Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt
ISSN-Print 2199-8906
ISSN-Internet 2199-8914

1. Auflage: 500 Stück
März 2017

Zitiervorschlag:
Eisele, Daniel et al. (2017): White Paper Privatheit in öffentlichen WLANs: Spannungsverhältnisse zwischen gesellschaftlicher Verantwortung, ökonomischen Interessen und rechtlichen Anforderungen. Hrsg.: Michael Friedewald et al., Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Karlsruhe: Fraunhofer ISI.

Druck
Stober GmbH Druck und Verlag, Eggenstein

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

PROJEKTPARTNER

Fraunhofer

Natur Technik Kultur Gesellschaft
UNIKASSEL VERSITÄT

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

UNIVERSITÄT HOHENHEIM
LEHRSTUHL FÜR MEDIENPSYCHOLOGIE

EBERHARD KARLS UNIVERSITÄT TÜBINGEN
INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein