Editorial – Grußwort des Forschungsprojektleiters »BayWiDI« Prof. Dr. Dirk Heckmann

Sehr geehrte Leserinnen und Leser,

herzlich willkommen zur zehnten Ausgabe des BayWiDI-Newsletters.

Das »Streitthema Tracking« ist spätestens mit dem Phänomen der personalisierten Online-Werbung elementarer Bestandteil der digitalen Gesellschaft geworden. Eine mehr als kontrovers diskutierte Thematik, die sowohl in der digitalen Sphäre als auch im analogen Leben allgegenwärtig ist und auch fortwährend sein wird. Jedenfalls aber ist die rechtliche Einordnung des Trackings spätestens seit Geltung der Datenschutzgrundverordnung um einiges unübersichtlicher geworden. Unser Beitrag auf Seite 2 bezieht sich deshalb insbesondere auf das Datenschutzrecht und auf den gegenwärtigen Entwurf der ePrivacy-Verordnung.

Unter der Überschrift »Der neue WPA3-Standard – gibt es eine Pflicht zur Aktualisierung?« finden Sie Informationen zum neuen WPA3-Standard, eine Entwicklung, die sich als besonders alltagsrelevant erweist. Gerade mit Blick auf eine im Jahr 2017 öffentlich gewordene gravierende Sicherheitslücke in der WLAN-Verschlüsselung WPA2 verspricht der neue Verschlüsselungsstandard die Lösung zahlreicher Sicherheitsprobleme. Der Beitrag auf Seite 5 behandelt alle Neuerungen und Vorteile der WPA3-Verschlüsselung und vor allem die rechtliche Frage, ob Nutzer verpflichtet sind, ihre Geräte auf die neue WPA3-Verschlüsselung umzurüsten.

»Weg frei für offenes WLAN«, »Mehr Rechtssicherheit für Anbieter« »Störerhaftung bleibt abgeschafft« – das ist lediglich eine kleine Auswahl der unzähligen Schlagzeilen, mit denen das Grundsatzurteil des BGH zur Haftung des Anschlussinhabers für Urheberrechtsverletzungen über ungesichertes WLAN (»Dead Island«) medial begrüßt worden ist. Während das Betreiben eines ungesicherten WLAN wegen der sogenannten Störerhaftung – einem Haftungsinstitut, dessen Existenz seit jeher stark umstritten war – in der Vergangenheit ein insbesondere finanzielles Risiko darstellte, sorgt das Urteil zukünftig für ein Mehr an Rechtssicherheit für zahlreiche Anschlussinhaber. Es bestätigt die seit 2017 geltende Rechtslage, die private und geschäftliche »Free WiFi«-Anbieter gleichermaßen von der Störerhaftung freistellt. Eine ausführliche Besprechung finden Sie ab Seite 8.

Um Deutschland besser gegen Cyberangriffe zu schützen, beschloss die Bundesregierung jüngst die Gründung einer »Cyberagentur« nach US-amerikanischem Vorbild. Wenngleich zahlreiche Details noch offen sind, steht bereits fest, dass die schon im Koalitionsvertrag von Union und SPD vereinbarte Cyberagentur unter der gleichberechtigten Führung von Innen- und Verteidigungsministerium stehen soll, denn die Gewährleistung der IT-Sicherheit von beispielsweise Krankenhäusern, Regierungsorganen oder der Bundeswehr könne nur gemeinsam sichergestellt werden. Dennoch trifft die Cyberagentur auch auf Bedenken, die sich etwa in Form der Forderung nach einer defensiven Ausrichtung der Agentur zeigen. Welche Aufgaben diese Cyberagentur letztlich haben wird, ist noch unklar. Sie sehen – es bleibt spannend!

Ich wünsche Ihnen viel Freude bei der Lektüre dieses Newsletters!

Ihr Prof. Dr. Dirk Heckmann,
Leiter des Forschungsprojekts »BayWiDI«

Inhalt

Tracking im Internet – quo vadis?

Die Problematik personalisierter Online-Werbung und der hierfür notwendige Einsatz von Tracking-Technologien wird schon seit vielen Jahren diskutiert.[1] Vielleicht auch wegen der konstanten Verbreitung solcher Praktiken in allen Lebensbereichen der digitalen Sphäre und auch der analogen Welt, wird diese Debatte aber in letzter Zeit aber vermehrt geführt. Individualisierte Werbung ist schon längst ein wichtiger Bestandteil der digitalisierten Gesellschaft. Dieser Beitrag befasst sich mit Tracking, seinen Vor- und Nachteilen, den rechtlichen Rahmenbedingungen und bereits absehbaren Entwicklungen.

Einleitung

Das wirtschaftliche Potenzial von Tracking beschränkt sich nicht nur auf interessenbasierte Werbung: Mithilfe der gewonnenen Erkenntnisse kann unter anderem auf Trends frühzeitig reagiert und sich den Wünschen der Nutzer angepasst werden. Tracking ist im Kern das Nachvollziehen des Nutzerverhaltens auf Webseiten[2] und umfasst sowohl die Erhebung als auch die Auswertung dieser Daten. Die Erhebung der Nutzerdaten erfolgt meist durch den Einsatz eines Tracking-Pixels. Das sind kleine – und für den Nutzer meist nicht zu erkennende – Grafiken, die automatisch aufgerufen werden, wenn eine E-Mail oder eine Webseite geöffnet wird. Tracking-Mechanismen können aber auch eindeutig sein wie beispielsweise ein Like-Button in einem sozialen Netzwerk. Durch solche Tracking-Mechanismen kann das Surfverhalten des Nutzers genau verfolgt werden: Suchanfragen, besuchte Webseiten und Einkäufe werden »getrackt«. Sogar die Mausbewegung, die meist der Augenbewegung entspricht,[3] wird verfolgt, um nachvollziehen zu können, was sich der Nutzer länger anschaut.

Diese Daten werden dann – meist von 3rd-Party-Web-Analytics-Systemen – ausgewertet, um detaillierte Echtzeitprofile der Nutzer zu erstellen. Diese Profile verraten höchst sensible Informationen über den Nutzer, von seiner ethnischen Herkunft über seine politische Ausrichtung bis hin zu seinem Einkommen, Drogenkonsum und seinen Interessen im Allgemeinen. Auf Grundlage dieser Daten kann die Wahrscheinlichkeit gewisser Handlungen des Nutzers in verschiedenen Situationen errechnet werden.[4]

Funktionsweise

Damit das Tracking und somit auch die Profilbildung webseiten-, webbrowser- und sitzungsübergreifend erfolgen kann, muss das genutzte Gerät wiedererkannt werden können. Bei browserbasierten Webangeboten werden z.B. zwei bekannte Wiedererkennungsmethoden verwendet: Cookies und Device Fingerprinting. Cookies sind kleine Textdateien, die vom Webserver auf dem Endgerät abgelegt werden. Sie enthalten eine eindeutige Cookie-ID, wodurch der Nutzer wiedererkannt werden kann.[5] Diese Methode hat allerdings aus Sicht der Tracker den Nachteil, dass Cookies jederzeit vom Nutzer gelöscht werden können. Demgegenüber ist Device Fingerprinting eine Methode, der sich der Nutzer nicht so leicht entziehen kann: Hierbei werden sämtliche Merkmale des Geräts, wie die Bildschirmauflösung, die Browsersprache, installierte Plugins und die Zeitzone des Nutzers ausgelesen und analysiert. Mithilfe dieser Auswertung kann ein »digitaler Fingerabdruck« des Endgeräts erstellt werden.[6] Im Gegensatz zu Cookies kann der Nutzer Device Fingerprinting nur schwer unterbinden: Es lassen sich zwar Plugins installieren, die bewirken, dass weniger Informationen über das Endgerät errechnet werden. Allerdings können diese Plugins genau das Gegenteil bewirken, denn auch solche Plugins sind ein Merkmal des Endgeräts und kann somit die Wiedererkennung ermöglichen.[7] Device Fingerprinting kann jedoch auch für beide Seite nützlich sein, wenn es zum Beispiel zur Betrugserkennung oder zum Spamschutz eingesetzt wird.[8]

1 Vgl. den im Tagesspiegel erschienenen Beitrag »Personalisierte Werbung: Durchs Netz verfolgt« aus dem Jahr 2012, https://www.tagesspiegel.de/wirtschaft/streitthema-tracking-personalisierte-werbung-durchs-netz-verfolgt-/6445032.html, abgerufen am 30.08.2018.

2 *Katsivelas*, in: Albers/Katsivelas (Hrsg.), Recht & Netz, 2018, S. 227 f.

3 *Völkel*, »Mousetracking & Eyetracking. Ein Blick, ein Klick: Erst gucken, dann klicken.«, https://www.scoreberlin.de/usability-artikel/mousetracking-eyetracking/, abgerufen am 30.08.2018.

4 *Richter*, DuD 2016, 581.

5 Ausführlich zur Funktionsweise *Krimphove/Michel*, ZVertriebsR 2017, 149.

6 *Conrad*, in: Handbuch Datenschutz und IT-Sicherheit, Teil E, Rn. 97.

7 »Device Fingerprinting – Wie funktioniert der digitale Fingerabdruck?«, https://www.datenschutzbeauftragter-info.de/device-fingerprinting-wie-funktioniert-der-digitale-fingerabdruck/, abgerufen am 30.08.2018.

8 *Lachenmann*, in: Formularhandbuch Da-

Cookies und Fingerprints ermöglichen jedoch nur ein gerätebezogenes Wiedererkennen. Damit das Cross-Device-Tracking, also das Widererkennen eines Nutzers über mehrere Endgeräte hinweg, gelingt, muss auf User-IDs oder Geräte-IDs zurückgegriffen werden. User-IDs entstehen, wenn sich ein Nutzer durch ein Login, etwa auf sozialen Netzwerken oder bei Online-Shops, oder durch eine Registrierung, beispielsweise für einen Newsletter, identifizieren lässt. Geräte-IDs sind komplexer zu ermitteln: Es müssen große Datenmengen erhoben und ausgewertet werden, um Zusammenhänge und Muster zu entdecken, die eine Zuordnung mehrerer Geräte zu einem Nutzer möglich machen.[9] Diese Methode ist allerdings nicht so treffsicher wie eine User-ID.

Einsatzmöglichkeiten

Die Einsatzmöglichkeiten solcher Methoden und der daraus gewonnenen Informationen im unternehmerischen Kontext sind sehr vielfältig. Zum einen gibt es die wohl bekannteste Verwendungsmöglichkeit, das Behavioral Targeting. Dabei handelt es sich um eine Methode im Online-Marketing, die eine individualisierte Ansprache des Nutzers auf Grundlage der gewonnenen Datenmengen bezüglich seines Verhaltens und seiner Persönlichkeit ermöglicht.[10] Diese individualisierte Werbung wird meist durch Programmatic Advertising verbreitet. Hierbei werden Plätze für Werbeanzeigen auf Webseiten anhand der Nutzerprofile automatisch und in Echtzeit auktioniert. Vonseiten des Nutzers kann es durchaus als vorteilhaft empfunden werden, vermehrt nur interessenbezogene Werbung angezeigt zu bekommen. Kritische Stimmen befürchten dagegen, dass durch eine solche personalisierte Ansprache das Nutzerverhalten beeinflusst und im schlimmsten Fall sogar gesteuert werden kann. Die mögliche Kontrolle des Nutzerverhaltens begrenzt sich nicht nur auf die Produkt- oder Markenauswahl, sondern kann auch eingesetzt werden, um Kaufanreize zu schaffen, zu erhöhen, hemmende Faktoren zu eliminieren und Vorlieben und Schwächen zu instrumentalisieren.[11] Letzteres lässt sich durch die Auswertung der über die Nutzer gewonnen Daten mithilfe von soziodemografischen Erkenntnissen erreichen.[12]

Durch Tracking können Unternehmen auch Informationen gewinnen, die bei der Webseitenoptimierung behilflich sein können. So kann beispielsweise ermittelt werden, wann Kunden den Bestellprozess abbrechen oder welche Elemente der Webseite schwer zu bedienen sind. Des Weiteren können Unternehmen gezielt und zeitgemäß auf die Begehren der Nutzer reagieren, indem sie Trends frühzeitig erkennen und ihre Produkte und Preise daran anpassen.

Kritik an Behavioral Targeting und Datenschutz

Doch Behavioral Targeting ist nicht unumstritten. Im politischen Bereich wird es häufig als Gefahr für die Demokratie gesehen, sowohl in internationalen wie auch in deutschen Wahlkämpfen. Auch im unternehmerischen Kontext stößt Behavioral Targeting auf Kritik: Es wird über das Missbrauchspotenzial solcher neuen Technologien aufgrund der Macht- und Informationsasymmetrie[13] diskutiert. Beispielsweise könne es zu manipulativen und ausbeuterischen Praktiken kommen. Journalisten haben beispielsweise aufgedeckt, dass Facebook deprimierte Jugendliche in Australien und Neuseeland als Zielgruppe für Werbung identifiziert hat.[14] Kritisch wird auch angemerkt, dass es zu einem Verlust der Privatautonomie führen könne, wenn der Betroffene in seiner Entschließungsfreiheit erheblich beeinträchtigt werde. Es bedürfe daher effektiver Instrumente zum Schutz der Nutzer.[15] Zudem wird auch die Gefahr der Preisdiskriminierung genannt,[16] wenn Unternehmen die Möglichkeit haben, unterschiedliche Preise für die gleichen Produkte zu verlangen, je nachdem, welcher Nutzer angesprochen wird. Auch das zugrundeliegende Tracking wird oft kritisiert, insbesondere wegen der Beeinträchtigung der Privatsphäre des Nutzers.

Die rechtliche Einordnung des Trackings ist spätestens seit Inkrafttreten der Datenschutz-Grundverordnung um einiges unübersichtlicher geworden: Vor dem 25.05.2018, dem Datum, zu dem die Datenschutz-Grundverordnung ihre Wirkung entfaltet hat, galt das deutsche Telemediengesetz als nationale Umsetzung der europäischen ePrivacy-Richtlinie. Gemäß § 15 Abs. 3 S. 1 TMG durften pseudonymisierte Nutzerprofile »für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien« erstellt werden. Hier-

tenschutzrecht, 2. Aufl. 2018, Teil F, S. 565.

9 »Cross-Device Tracking«, https://de.ryte.com/wiki/Cross-Device_Tracking, abgerufen am 30.08.2018.

10 *Ebers*, MMR 2018, 423.

11 *Richter*, DuD 2016, 581; *Ebers*, MMR 2018, 423.

12 *Katsivelas*, in: Albers/Katsivelas (Hrsg.), Recht & Netz, 2018, S. 227.

13 *Ebers*, MMR 2018, 423, 424.

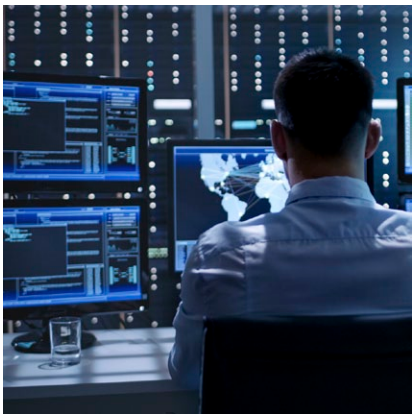
14 *Reilly*, »Is Facebook Targeting Ads at Sad Teens?«, https://www.technologyreview.com/s/604307/is-facebook-targeting-ads-at-sad-teens/, abgerufen am 30.08.2018.

15 *Ebers*, MMR 2018, 423, 428.

16 *Hofmann*, WRP 2016, 1074.

bei galt das Opt-Out-Prinzip, der Nutzer musste einer Profilbildung also aktiv widersprechen, worauf er deutlich hinzuweisen war. Die europäische Datenschutz-Grundverordnung genießt jedoch Anwendungsvorrang vor dem deutschen Telemediengesetz und verdrängt – trotz der Kollisionsregel des Art. 95 DS-GVO – die einschlägigen Vorschriften des Telemediengesetzes.[17] Weil die ePrivacy-Richtlinie nicht unmittelbar angewendet werden kann,[18] gelten vorerst nur die Bestimmungen der Datenschutz-Grundverordnung.

Diese besagen, dass die Verarbeitung personenbezogener Daten grundsätzlich verboten und nur in bestimmten Fällen ausnahmsweise erlaubt ist. Als Erlaubsnisgrundlagen kommen entweder berechtigte Interessen des für das Tracking Verantwortlichen gem. Art. 6 Abs. 1 lit. f) DS-GVO oder eine Einwilligung des Nutzers gem. Art. 6 Abs. 1 lit. a) DS-GVO in Betracht. Die berechtigten Interessen des Verantwortlichen, zu denen auch das Onlinemarketing zählt, könnten die Verarbeitung personenbezogener Daten grundsätzlich rechtfertigen. Allerdings dürfen keine schutzwürdigeren Interessen des Nutzers, wie etwa der Schutz seiner Privatsphäre, die Interessen des Verantwortlichen überwiegen. Eine reine Reichweitenanalyse oder Webseiten-Optimierung wären Beispiele für einen Fall, in dem keine Profile von einzelnen Nutzern gebildet und Daten pseudonymisiert oder anonymisiert werden.[19] In anderen Fällen besteht ein Einwilligungserfordernis i.S.d. Datenschutz-Grundverordnung (vgl. Art. 7 DS-GVO). Dementsprechend muss der Nutzer eine informierte, freiwillige und widerrufbare Einwilligung erteilen. Dieses Opt-In-Prinzip bildet das Gegenstück zu der Regelung des Telemediengesetzes.



Die noch im Entstehen befindliche ePrivacy-Verordnung soll die ePrivacy-Richtlinie ablösen und ein einheitliches Datenschutzrecht für elektronische Kommunikation[20] schaffen. Auch auf Wiedererkennungsmethoden wie Cookies oder Device Fingerprinting sollen die ePrivacy-Regelungen, sowohl der Richtlinie wie auch des Verordnungsentwurfs, Anwendung finden.[21] Es handelt sich nämlich um Methoden, die auf endgerätebezogener Datenverarbeitungen basieren und entweder Informationen im Endgerät des Nutzers speichern (Cookies) oder Zugriff auf Informationen nehmen, die im Endgerät des Nutzers gespeichert sind (Device Fingerprinting).[22]

Nach dem jetzigen Stand des Entwurfs der ePrivacy-Verordnung wird die Integrität des Endgeräts des Nutzers umfassend geschützt (vgl. Art. 8–10),[23] auch das Errechnen eines digitalen Fingerabdrucks wäre von einer Einwilligung des Nutzers abhängig.

Die ePrivacy-Verordnung befindet sich noch im Entwurfsstadium. Doch selbst nach ihrem Inkrafttreten wird es höchstwahrscheinlich noch eine einjährige Übergangsfrist geben, wie sie der LIBE-Ausschuss vorgeschlagen hat. Somit liegen der gegenwärtige Stand und der zu erwartende Fortschritt weit hinter dem eigentlich geplanten zeitgleichen Inkrafttreten von Datenschutz-Grundverordnung und ePrivacy-Verordnung zurück.

Allerdings drängen die technologischen Fortschritte in diesem Bereich auf eine zügige Regelung: Microsoft hat beispielsweise ein Patent angemeldet, das den emotionalen Zustand des Nutzers ermitteln können soll. Unternehmen könnten damit ihre Werbung gezielt auf eine Stimmung des Nutzers hin optimieren.[24] Weiterhin wird das Offline-Conversion-Tracking insbesondere durch Facebook und Google[25] immer weiter ausgebaut, um beispielsweise verfolgen zu können, ob eine Online-Werbung zu einem Offline-Kauf geführt hat. Dazu können Standort-, Bluetooth- oder WLAN-Daten eingesetzt werden. Australische Forscher behaupten sogar, dass sie durch die Fingerbewegungen auf Touchscreens die Nutzer wiedererkennen können.[26] Es ist zu erwarten, dass solche Entwicklungen, die die Integrität der Endgeräte und die Privatsphäre der Nutzer gefährden, weiter vorangetrieben werden.

Kitur

17 Positionsbestimmung der Datenschutzkonferenz vom 26.04.2018, »Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018«, https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf, abgerufen am 30.08.2018. Anderer Ansicht ist *Hanloser*, ZD 2018, 213, 216.

18 Vgl. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM%3Al14547.

19 *Schwenke*, »Datenschutz und ePrivacy 2018 – Änderungen für Onlinemarketing, Tracking und Cookies«, https://drschwenke.de/datenschutz-eprivacy-online-marketing-cookies/#Berechtigte_Interessen_als_Erlaubnisgrundlage, abgerufen am 30.08.2018.

20 Erwägungsgrund 5 des Entwurfs einer ePrivacy-Verordnung in der Fassung des Rats der Europäischen Union vom 04.05.2018, Dokument ST 8537 2018 INIT, abzurufen unter http://data.consilium.europa.eu/doc/document/ST-8537-2018-INIT/en/pdf.

21 Art. 5 Abs. 3 ePrivacy-Richtlinie und Art. 2 Abs. 1 lit. b) des Entwurfs einer ePrivacy-Verordnung.

22 *Conrad*, in: Handbuch Datenschutz und IT-Sicherheit, Teil E, Rn. 98.

23 Vgl. *Hanloser*, ZD 2018, 213, 217.

24 Google Patents, »Targeting Advertisements Based on Emotion«, https://patents.google.com/patent/US20120143693A1/en, abgerufen am 30.08.2018.

25 Vgl. Facebook, »Offline-Conversions«, https://www.facebook.com/business/help/www/1782327938668950 und Google Ads, »Offline-Conversion-Tracking«, https://support.google.com/google-ads/answer/2998031?hl=de, abgerufen am 30.08.2018.

26 *Masood u.a*, Proceedings on Privacy Enhancing Technologies 2018, 122.

Der neue WPA3-Standard – gibt es eine Pflicht zur Aktualisierung?

Nachdem im Herbst 2017 eine »gravierende Sicherheitslücke«[1] in der WLAN-Verschlüsselung WPA2 bekannt wurde, wurde auf der CES[2] im Januar 2018 der neue Verschlüsselungsstandard WPA3 vorgestellt. WPA3 soll den Datenaustausch von Netzwerkgeräten mit dem WLAN-Access-Point noch sicherer machen und so vor unberechtigter Nutzung durch Dritte schützen. In diesem Beitrag sollen die bisher verbreitete WPA2-Verschlüsselung und anschließend die Neuerungen und Vorteile der WPA3-Verschlüsselung kurz erklärt werden.

Anschließend wird der Frage nachgegangen, ob WLAN-Nutzer rechtlich verpflichtet sein werden, ihre Router auf die neue WPA3-Verschlüsselung umzurüsten.

1. Funktionsweise der WPA2-Verschlüsselung

WPA2, die Kurzform für Wi-Fi Protected Access 2, ist einer von mehreren Verschlüsselungsmethoden[3] für WLAN. Bisher war WPA2 der sicherste Standard.[4] WPA2 verwendet das Sicherungsprotokoll CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), das auf dem Verschlüsselungsalgorithmus AES (Advanced Encryption Standard) basiert. Das ist ein Algorithmus für die dynamische Blockverschlüsselung, auch »Blockchiffre« genannt. Dabei werden Daten in Blöcken verschlüsselt und später entschlüsselt. Der CCMP-Sicherheitsstandard ist ein symmetrisches Verfahren, bei dem alle Kommunikationspartner einen gemeinsamen Schlüssel nutzen (»Pairwise Master Key«, PMK).[5] Das Verfahren funktioniert daher nur, wenn sowohl der Absender als auch der Empfänger der Daten denselben geheimen Schlüssel kennen.[6] Den WPA2-Standard gibt es in zwei unterschiedlichen Ausführungen: In der »Personal«-Version nutzen alle Anwender ein vorher vergebenes Passwort (»Pre-Shared Key«, PSK), bei »Enterprise« wird für jeden Anwender auf einem Authentifizierungsserver ein Benutzerkonto mit individuellem Schlüssel hinterlegt.[7]

2. Sicherheitslücken in WPA2

Trotz des sehr hohen Sicherheitsstandards ist im Herbst 2017 eine bedeutsame Sicherheitslücke in der WPA2-Verschlüsselung bekannt geworden. Durch eine Schwachstelle ist es möglich, ohne Kenntnis des Passworts die Kommunikation mitzulesen.[8] Diese Sicherheitslücke ist von den Sicherheitsforschern *Mathy Vanhoef* und *Frank Piessens* entdeckt und dokumentiert worden.[9] Die »Key Reinstallation Attack« genannte Angriffsmethode nutzt unter anderem eine Schwachstelle in der bis dahin als sicher geltenden Authentifizierungsmethode, dem sog. »(4-Way)-Handshake«.[10] Der 4-Way-Handshake arbeitet mit gegenseitigen Authentifizierungsschlüsseln. In einem in vier Schritte unterteilten Prozess bestätigen sich der WLAN-Access Point und das WLAN-Netzwerkgerät gegenseitig, den gemeinsamen Pairwise Master Key zu kennen. In diesem Verfahren wird auch der gemeinsam genutzte Sitzungsschlüssel festgelegt.[11]

Die Umgehung der 4-Way-Handshake-Authentifizierung gelingt durch die

1 *Lewalter*, Computerbild, http://www.computerbild.de/artikel/cb-News-Sicherheit-Verschluesselungsprotokoll-WPA3-Infos-19609207.html, abgerufen am 30.08.2018.

2 Die Consumer Electronics Show, kurz CES, ist eine Technik-Messe in Las Vegas.

3 So existieren etwa auch WEP, WPA und WPA+WPA2, vgl. *Khunkham*, Welt, https://www.welt.de/wirtschaft/webwelt/article135694274/Welche-Verschluesselung-macht-mein-WLAN-schneller.html, abgerufen am 30.08.2018.

4 *Eichfelder*, Chip, https://praxistipps.chip.de/wpa2-verschluesselung-die-besten-tipps_19552, abgerufen am 30.08.2018.

5 *BSI*, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02388.html, abgerufen am 30.08.2018.

6 *Rouse*, SearchSecurity, https://www.searchsecurity.de/definition/Advanced-Encryption-Standard-AES, abgerufen am 30.08.2018.

7 *Behrens*, PCWelt, https://www.pcwelt.de/ratgeber/WLAN-Verschluesselung-erklaert-Ratgeber-Sicherheit-365720.html, , abgerufen am 30.08.2018.

8 *Gierow/Grüner*, Golem, https://www.golem.de/news/wlan-wpa-2-ist-kaputt-aber-nicht-gebrochen-1710-130636.html, abgerufen am 30.08.2018.

9 *Vanhoef/Piessens*, Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, https://papers.mathyvanhoef.com/ccs2017.pdf, abgerufen am 30.08.2018.

10 *Vanhoef/Piessens*, Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, S. 1.

11 *Schirrmacher*, Heise, https://www.heise.de/security/meldung/Details-zur-KRACK-Attacke-WPA2-ist-angeschlagen-aber-nicht-gaenzlich-geknackt-3862571.html, abgerufen am 30.08.2018.

nochmalige Installation eines in diesem Verfahren festgelegten Sitzungsschlüssels (»Pairwise Transient Key«, PTK). Der Angreifer schaltet sich hierfür zwischen die Kommunikation von Sitzungsschlüssel-Anfrager und Authentifizierer (»Man in the Middle«) und installiert den – eigentlich bereits installierten – Sitzungsschlüssel erneut.[12] Der neu installierte Schlüssel ist dann der Sitzungsschlüssel, der für die CCMP-Verschlüsselung genutzt wird. In der Folge lassen sich sämtliche gesendeten Datenpakete entschlüsseln.[13] Der Erfolg dieses Angriffs beruht auf der Designschwäche von WPA2, eine erneute Installation eines – bereits installierten – Schlüssels nicht zu verhindern.[14]

Diese Angriffsmethode funktioniert in allen Varianten der WPA2-Verschlüsselung[15] und konnte auch erfolgreich für die Umgehung der ohnehin schon unsichereren Verschlüsselungsstandards WEP und WPA eingesetzt werden. Insgesamt sind sämtliche Systeme für die Key Reinstallation-Angriffe anfällig. Linux und Android-Systeme sind wohl besonders gefährdet, bisher soll es aber keinen Angriff nach dieser Methode gegeben haben.[16]

Die Gefährdung ist jedoch insgesamt geringer, als es zu erwarten ist. Die Sicherheitslücke kann nämlich bei WPA2 durch entsprechende Updates behoben werden. Diese stehen zwar bisher nicht für jedes Gerät zur Verfügung,[17] Linux- und Windows-Nutzern ist allerdings bereits eine Patch-Lösung für die WPA2-Verschlüsselung angeboten worden. Auch Apple hat Updates in Aussicht gestellt.[18]

Zu Beginn des vergangenen Monats haben Sicherheitsforscher einen weiteren Mangel im WPA2-Standard bekannt gemacht, der überdies durch eine direkte Kommunikation mit dem Access-Point erfolgen kann (»client-less« attack). Nach dieser Methode ist es nicht mehr notwendig, den gesamten 4-Way-Handshake zwischen Nutzer und Access-Point zu erfassen.[19] Die Entdecker gehen davon aus, dass diese Angriffsmethode alle Geräte betrifft.[20]

3. Neuerungen der WPA3-Verschlüsselung

Eine neuartige Variante der Verschlüsselung soll nun der WPA3-Standard liefern. Die Wi-Fi-Alliance, ein weltweites Firmenkonsortium bestehend aus verschiedenen Chip- und Geräteherstellern, stellte in Las Vegas WPA3 als Teil eines stärkeren Schutzmechanismus' vor, der selbst display-lose Geräte oder Geräte mit nur schwachem Passwortschutz schützen können soll.[21] Der Schutz von Geräten ohne Benutzeroberfläche ist besonders für Internet-of-Things-Geräte (IoT)[22] interessant, da hier eine WLAN-Verbindung meist nur per Knopfdruck aufgebaut wird und weitere Konfigurationen durch den Nutzer nicht möglich sind.[23] Der Hauptunterschied von WPA3 zu seinen Vorgängern besteht darin, dass WLAN-Router und Access-Points nach dem älteren Verschlüsselungsstandard einen gemeinsam Sitzungsschlüssel für alle Nutzer ihrer Funkzellen verwenden. Bei WPA3 hingegen soll jedem Nutzer ein eigener Schlüssel zugeordnet werden.[24] WPA3 arbeitet zudem mit einer modifizierten Verschlüsselungs- und Authentifizierungmethode, was die bei WPA2 noch angreifbare Handshake-Methode verbessern soll.[25] Ein Key Reinstallation-Angriff soll dann nicht mehr möglich sein.[26]

Die robustere Authentifizierung und verbesserte Kryptografie schließt sogar ausdrücklich alte, unsichere Protokolle aus.[27] Bisher konnten bei der Verwendung von WPA2 durch sog. Wörterbuch-Angriffe, bei denen eine Vielzahl von Zeichenkombinationen als Passwörter ausprobiert werden, schwache Passwörter überwunden werden. Die Einführung der neuen Verfahrensmethode (Simultaneaous Authentication of Equals, SAE) beabsichtigt, dieses Vorgehen stark zu erschweren.[28] Dass der neue WPA3-Standard deutlich schwerer zu überwinden ist als der WPA2-Standard, haben auch die Entdeckter des »client-less«-An-

12 *Vanhoef/Piessens*, Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, S. 5.

13 *Vanhoef/Piessens*, Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, S. 5.

14 *Schirrmacher*, Heise.

15 *Vanhoef / Piessens*, Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, S. 1.

16 *Schirrmacher*, Heise.

17 *Schwimmbeck/Humpa*, Chip, https://www.chip.de/news/WLAN-Verschluesselung-WPA2-geknackt-So-schuetzen-Sie-Ihr-WLAN-Netz-jetzt_125394046.html, abgerufen am 30.08.2018.

18 *Becker*, Heise, https://www.heise.de/mac-and-i/meldung/KRACK-Attacke-Apple-stellt-baldige-Updates-in-Aussicht-3864990.html, abgerufen am 30.08.2018.

19 *Zivadinovic*, Heise, https://www.heise.de/newsticker/meldung/WPA2-und-WLAN-Sicherheit-Direkter-Angriff-auf-WLAN-Router-4130759.html, abgerufen am 30.08.2018.

20 *Zivadinovic*, Heise.

21 *Wi-Fi Alliance*, https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements, abgerufen am 30.08.2018.

22 Eine zusammenfassende Erklärung des Internet of Things gibt *Litzel*, https://www.bigdata-insider.de/was-ist-das-internet-of-things-a-590806/ abgerufen am 30.08.2018.

23 *Pastorino*, welivesecurity, https://www.welivesecurity.com/deutsch/2018/02/12/wpa3-verbesserte-wlan-sicherheit/, abgerufen am 30.08.2018.

24 *Zivadinovic*, Heise.

25 *Pastorino*, welivesecurity.

26 *Wi-Fi Alliance*.

27 *Zivadinovic*, Heise.

28 *Zivadinovic*, Heise.

griffs auf die WPA2-Verschlüsselung zugestanden.[29]

Der zukünftige Nutzen von WPA3 kann zu diesem frühen Zeitpunkt kaum vorhergesehen werden. Die Auslieferung der ersten WPA3-fähigen Geräte ist erst für Ende 2018 geplant. Die Entwickler sehen in WPA3 jedoch eine Verschlüsselungsoption, die in Zukunft verstärkt genutzt werden wird.[30] Besonders eignen soll sich WPA3 für Einrichtungen mit besonders hohen Sicherheitsanforderungen – hingegen könnten private Nutzer, bei entsprechend regelmäßigen Updates, womöglich bereits mit dem WPA2-Standard hinreichend abgesichert sein.[31]

3. Rechtliche Bewertung

Die Frage, ob Geräte mit WPA2-Standard bald auf WPA3 aktualisiert werden müssen, stellt sich nicht nur aus der Perspektive der IT-Sicherheit, sondern auch aus rechtlicher Sicht. Wenn es eine rechtliche Pflicht zur Aktualisierung gibt, könnte das Beibehalten des alten WPA2-Standards zu einem rechtlichen Haftungsrisiko führen.

Der Ausgangspunkt für diese mögliche Haftung ist die sogenannte Störerhaftung, bei der ein eigentlich unbeteiligter Dritter für die Rechtsverletzung eines anderen haftet, wenn er willentlich und adäquat-kausal zur Verletzung eines geschützten Rechtsgutes beigetragen hat.[32] Für einen solchen Beitrag genügte es – nach alter Rechtslage – beispielsweise, Dritten den Zugriff auf ein unverschlüsseltes WLAN zu ermöglichen. Die bekanntesten Fälle sind die, bei denen ein ungesichertes WLAN für Filesharing genutzt wurde.[33]

Die Rechtsprechung hatte in einer Reihe von Entscheidungen die Verpflichtung von WLAN-Anbietern entwickelt, sei-

29 *Zivadinovic*, Heise.

30 *Wi-Fi Alliance*.

31 Vgl. etwa: *Kolkmann*, GIGA, https://www.giga.de/extra/wlan/specials/wpa3-verschluesselung-alles-zum-neuen-sicherheitsstandard/, abgerufen am 30.08.2018.

32 *BGH*, MMR 2004, 668.

33 Vgl. für eine ausführlichere Darstellung mit weiteren Hinweisen *Härting*, Internetrecht, 6. Aufl. 2017, Rn. 2728 ff., 2247 ff., dort auch zum Folgenden.

en es private oder geschäftliche, für eine Verschlüsselung ihres WLAN zu sorgen. Anderenfalls mussten sie damit rechnen, als Störer für Rechtsverletzungen zu haften, die Dritte über ihr ungesichertes oder nicht hinreichend gesichertes WLAN begangen hatten.[34] Als hierfür zu beachtender Sicherheitsstandard galt zumindest bei Privaten bisher, dass zum Zeitpunkt des Erwerbs des Routers marktübliche Sicherungen eingesetzt werden mussten. Die WPA2-Verschlüsselung erfüllte bisher diesen Standard. Mit Ankündigung der WPA3-Verschlüsselung könnte nun WPA3 als neuer marktüblicher Standard beim Neukauf von Geräten erforderlich werden.

Allerdings wurde die Störerhaftung für die Übertragung fremder Daten mit dem am 29.06.2017 verabschiedeten 3. TMG-Änderungsgesetz abgeschafft (hierzu ausführlich *Lorenz*, Grundsatzurteil des BGH zur Haftung des Anschlussinhabers für Urheberrechtsverletzungen über ungesichertes WLAN, in diesem Newsletter Seite 8). Seither können WLAN-Anbieter nicht mehr für Rechtsverletzungen, die Dritte über ihren Internetzugang begangen haben, auf Schadensersatz, Beseitigung, Unterlassung und auch nicht für Abmahnkosten in Anspruch genommen werden. Der Wegfall der Störerhaftung bedingt damit auch den Wegfall des Erfordernisses, eine unberechtigte Nutzung des WLAN durch marktübliche Sicherungen zu erschweren. Diese weitreichende Privilegierung gilt sowohl für private als auch geschäftliche WLAN-Anbieter.[35] Im Ergebnis erscheint aus haftungsrechtlicher Sicht ein Umsteigen auf die WPA3-Verschlüsselung zumindest nach der neuen Rechtslage nicht erforderlich zu sein.

In Betracht kommt lediglich, dass WLAN-Anbieter im Rahmen des neu geschaffenen Anspruchs nach § 7 Abs. 4 TMG zu Sperrmaßnahmen verpflichtet werden können. Als solche kommt gegebenenfalls auch eine Verschlüsselung in Betracht. Der dann erforderliche Standard könnte sich an der bisherigen Rechtsprechung zur Störerhaftung orientieren. Dafür müsste aber zunächst der Anspruch auf Einrichtung von Sperrmaßnahmen geltend gemacht werden. Das ist nur dann möglich, wenn es zu einer Rechtsverletzung gekommen und der eigentliche Rechtsverletzer nicht auszumachen ist. Eine grundsätzlich präventive Verschlüsselung ist jedenfalls nicht notwendig.

34 Vgl. für eine ausführlichere Darstellung mit weiteren Hinweisen *Härting*, Internetrecht, Rn. 2728 ff., 2247 ff., dort auch zum Folgenden.

35 *Spindler*, in: Spindler/Schmitz, TMG Kommentar, 2. Aufl. 2018, § 8 Rn. 26.

4. Fazit

WPA3 beseitigt einige Sicherheitslücken des WPA2-Standards und bietet somit eine gesteigerte IT-Sicherheit. Aus rechtlicher Perspektive gibt es jedoch bisher keinen Grund für einen Umstieg auf WPA3. Das ist weitgehend der Abschaffung der Störerhaftung im Bereich der Datenübertragung zu verdanken. Eine gesonderte WLAN-Verschlüsselung ist seither nicht mehr erforderlich. In Betracht käme einzig, dass ein Anspruch auf Verschlüsselung nach WPA3 als Sperrmaßnahme gem. § 7 Abs. 4 TM geltend gemacht werden könnte. Allerdings müsste das dem Verhältnismäßigkeitsgrundsatz[36] gerecht werden.

Zerbst, LL.M. (VUW)

36 Hierzu *Spindler*, in: Spindler/Schmitz, TMG Kommentar, 2. Aufl. 2018, § 7 Rn. 96.

Grundsatzurteil des BGH zur Haftung des Anschlussinhabers für Urheberrechtsverletzungen über ungesichertes WLAN

Offene WLAN-Hotspots sind hoch begehrt. Insbesondere Cafés sowie der stationäre Einzelhandel werben zunehmend mit »Free WiFi« um Kundschaft. Hierbei drängt sich eine zentrale Frage auf: Müssen Gastronomen, Handelsunternehmen, öffentliche Stellen oder sonstige Anbieter dafür haften, wenn ihr öffentlich zugängliches WLAN für rechtwidrige Handlungen genutzt wird?

In der Vergangenheit war der Betrieb eines ungesicherten WLAN aufgrund der sogenannten Störerhaftung vor allem aus finanzieller Sicht risikobehaftet. Nutzten Dritte den Internetzugang für Filesharing, konnte der Anbieter des WLAN abgemahnt und als Störer auf Unterlassung in Anspruch genommen werden. Ein Störer ist laut BGH jeder, der die Tat zwar nicht begangen, sie aber ermöglicht hat.[1] Dieses Haftungsinstitut sorgte dafür, dass frei zugängliches WLAN nur sehr vereinzelt betrieben wurde, zu groß war die Angst vor Abmahnkosten. Umfragewerten zufolge schrecken 59 % der befragten geschäftlichen und privaten Nutzer wegen Haftungsrisiken und 43 % wegen Sicherheitsbedenken davor zurück, einen für jedermann zugänglichen Hotspot anzubieten.[2]

Hierauf reagierte der Gesetzgeber vergangenes Jahr mit einer Änderung des Telemediengesetzes (TMG)[3]: Wer einen öffentlichen Zugang zum Internet bereitstellt, kann nun für rechtswidrige Handlung eines Nutzers weder auf Schadensersatz, Beseitigung noch Unterlassung in Anspruch genommen werden.

Zu dieser seit dem 13.10.2017 geltenden Regelung nahm nun der unter anderem für Urheberrecht zuständige Erste Zivilsenat des BGH in einem Grundsatzurteil vom 26.07.2018 (Az. I ZR 64/17 – Dead Island)[4] Stellung. Erstmalig befassten sich die obersten Zivilrichter mit der neuen Rechtslage und sprachen sich für deren (Europa-)Rechtskonformität aus. In dieser mit Spannung erwarteten Entscheidung klärten sie zahlreiche offene Fragen und legten einige Gesetzespassagen, die sie für unklar hielten, im Sinne des EU-Rechts aus.

1. Sachverhalt und bisheriger Prozessverlauf

In dem vom BGH entschiedenen Fall aus dem Jahr 2013 ging es um das Computerspiel »Dead Island«, das auf einer Tauschbörse unrechtmäßig von einem nicht zu ermittelnden Unbekannten zum Download angeboten worden war. Die Inhaberin der ausschließlichen Nutzungsrechte an dem Spiel, die Klägerin, hatte den Beklagten, über dessen Internetanschluss das Spiel angeboten wurde, auf Unterlassung und Erstattung der Abmahnkosten in Anspruch genommen. Ferner forderte sie ihn zur Abgabe einer strafbewehrten Unterlassungserklärung auf und verlangte Schadensersatz. Bei dem genutzten Internetzugang handelte es sich um ein frei zugängliches, nicht passwortgeschützten WLAN sowie einen Ausgangspunkt des anonymen Tor-Netzes (Tor-Exit-Node).

Tor-Netzwerke basieren auf dem technischen Prinzip des Onion Routing, bei dem Anfragen auf wechselnden Routen über verschiedene Server umgeleitet werden, die das eigentliche Ziel nicht kennen.[5] Im Anschluss an das Passieren der Stationen gelangt die Kommunikation sodann über einen Exit-Knoten zurück ins »offene« Internet. Der Kommunikationsvorgang ähnelt folglich einer Zwiebel bzw. deren Schichten (engl. onion). Das Surfen mittels eines Tor-Browsers bezweckt, die Anonymität von Sender und Empfänger sicherzustellen.

Bereits zweimal zuvor war der Beklagte von der Klägerin wegen im Jahr 2011 über seinen Internetanschluss begangener Urheberrechtsverletzungen durch Filesharing abgemahnt worden. Der Beklagte machte geltend, selbst keine Rechtsverletzung begangen zu haben.

Sowohl das Landgericht als auch das Berufungsgericht, das OLG Düsseldorf, gaben der Klägerin recht. Der Beklagte wurde dazu verurteilt, Dritte daran zu hindern, das Computerspiel oder Teile davon der Öffentlichkeit mittels seines Internetanschlusses über eine Internettauschbörse zur Verfügung zu stellen.

Beide Gerichte urteilten noch vor Inkrafttreten des dritten Gesetzes zur Änderung des TMG. Der BGH änderte das Urteil des Oberlandesgerichts nun entsprechend der Neuregelung ab.

1 Vgl. BGH v. 11.03.2004, Az. I ZR 304/01.

2 *Bundesministerium für Wirtschaft und Energie*, Mehr Rechtssicherheit bei WLAN, https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/wlan.html, zuletzt abgerufen am 30.08.2018.

3 Drittes Gesetz zur Änderung des Telemediengesetzes vom 28.09.2017 (BGBl. I 2017 S. 3530). Vgl. zur Reichweite der Änderungen des 3. TMG-Änderungsgesetzes beispielsweise *Sesing/Baumann*, MMR 2017, 583.

4 BGH v. 26.07.2018, Az. I ZR 64/17. Vorinstanzen: LG Düsseldorf v. 13.01.2016, Az. 12 O 101/15 sowie OLG Düsseldorf v. 16.03.2017, Az. I-20 U 17/16.

5 *Kupke*, Haften Tor-Helfer für Urheberrechtsverletzungen Dritter?, 21.06.2018, http://www.spiegel.de/netzwelt/web/bundesgerichtshof-haften-tor-helfer-fuer-urheberrechtsverletzungen-dritter-a-1214139.html, zuletzt abgerufen am 30.08.2018.

2. Entscheidung des BGH

Die obersten Zivilrichter hoben das vorausgehende Urteil des OLG Düsseldorfs hinsichtlich der Verurteilung zur Unterlassung auf und verwiesen die Sache zur erneuten Verhandlung an dieses zurück. Der Anbieter eines Internetzugangs über WLAN und eines Tor-Exit-Nodes[6] hafte nach § 8 Abs. 1 Satz 2 TMG nicht als Störer für von Dritten über seinen Internetanschluss im Wege des Filesharings begangene Urheberrechtsverletzungen.

Doch auch die Interessen der Rechtsinhaber will das neue TMG schützen. § 7 Abs. 4 TMG sieht vor, dass je nach Art und Schwere des Verstoßes WLAN-Anbieter zu einer Registrierung der Nutzer, einer Verschlüsselung des Zugangs mit Passwort oder im äußersten Fall sogar zu einer vollständigen Sperrung des Zugangs verpflichtet werden können.[7] Ferner besteht die (mildere) Möglichkeit, den Zugang zu Filesharing-Diensten zu sperren. Obgleich Diensteanbieter nach § 8 Abs. 3 TMG von einer Behörde nicht zu derartigen Maßnahmen verpflichtet werden dürfen, ist den Gerichten eine solche Verpflichtung des WLAN-Anbieters nach § 8 Abs. 3 TMG und (erst Recht) anderer Diensteanbieter nach § 8 Abs. 1 TMG möglich.[8]

Mit der Einführung eines Anspruchs auf Sperrmaßnahmen bezweckt der nationale Gesetzgeber, die Vorgaben des EuGH aus den Rechtssachen UPC Telekabel und McFadden umzusetzen, die sich auf Art. 8 Abs. 3 InfoSoc-Richtlinie (2001/29/EG) sowie Art. 11 Satz 3 Enforcement-Richtlinie (2004/48/EG) beziehen.[9] Im Gegensatz zum Referentenentwurf, der Zugangssperren lediglich als ein Beispiel nannte, sieht das neue TMG diese Sperren als einzig mögliches Mittel vor.[10]

Die BGH-Richter hielten die Sperrung von Internetangeboten für grundsätzlich rechtskonform, da nur so wiederholte Rechtsverletzungen vermieden werden könnten. In der Urteilsbegründung heißt es: Die Sperrung von Filesharing-Software sei technisch möglich und dem Beklagten zumutbar.[11] Die Entscheidung, ob der Klägerin tatsächlich der Anspruch zusteht, vom WLAN-Betreiber die Einrichtung von Sperrmaßnahmen zu verlangen, obliegt nun dem Oberlandesgericht als Tatsacheninstanz.

Hinsichtlich der Ausgestaltung dieser Sperrmaßnahmen äußerte sich der BGH nur vage. Feststünde, dass ein solcher Anspruch nicht auf eine bestimmte Technik beschränkt sei.[12] Voraussetzung sei aber stets, dass der Rechteinhaber keine andere Möglichkeit habe, der Verletzung seines Rechts abzuhelfen. Ferner müsse die Sperrmaßnahme zumutbar und verhältnismäßig sein[13], um sogenanntes Overblocking zu vermeiden.

Indes sah der BGH davon ab, den Gerichtshof der Europäischen Union (EuGH) im Rahmen eines Vorabentscheidungsverfahren hinzuzuziehen. Das sei nur bei Zweifeln über die Europarechtskonformität angezeigt. Die Karlsruher Richter aber beurteilten § 8 Abs. 2 Satz 2 TMG als europarechtskonform.[14] Hinsichtlich der Einschränkungen der Durchsetzung von Rechten des geistigen Eigentums sahen sie keine durchgreifenden unionsrechtlichen Bedenken. Zwar seien die Mitgliedstaaten nach europäischem Recht verpflichtet, gerichtliche Maßnahmen zu Gunsten der Rechteinhaber vorzusehen (Art. 8 Abs. 3 InfoSoc-Richtlinie und Art. 11 Satz 3 Enforcement-Richtlinie), jedoch sei die durch § 8 Abs. 1 Satz 2 TMG entstandene Rechtsschutzlücke richtlinienkonform dahingehend fortzubilden, dass der Sperranspruch gem. § 7 Abs. 4 TMG auch gegenüber den Anbietern drahtgebundener Internetzugänge geltend gemacht werden könne.[15] Damit verbliebe den geschädigten Rechteinhabern die Möglichkeit, WLAN-Betreiber gerichtlich zur Sperrung von Inhalten zu verpflichten[16], wodurch ihre (Urheber-)Rechte ausreichend geschützt werden würden. Mit Ausnahme des Falls,

6 Tor steht abkürzend für »The Onion Router Project« und meint ein Anonymisierungsnetzwerk.

7 Vgl. Rn. 54 der BGH-Entscheidung.

8 Vgl. Rn. 54 ff. der BGH-Entscheidung m.w.N.

9 *Spindler*, NJW 2017, 2305, 2305 m.w.N.

10 Ebd.

11 Vgl. Rn. 14 der BGH-Entscheidung.

12 Vgl. Rn. 54 der BGH-Entscheidung.

13 Vgl. Rn. 52 der BGH-Entscheidung.

14 Vgl. Rn. 58 der BGH-Entscheidung.

15 Vgl. Rn. 49 der BGH-Entscheidung.

16 Vgl. Rn. 54 der BGH-Entscheidung.

dass sich der WLAN-Betreiber absichtlich an einer Rechtsverletzung beteiligt, besteht somit kein Anspruch der Rechteinhaber auf die Erstattung außergerichtlicher oder gerichtlicher Kosten.[17]

Keiner Entscheidung des BGH bedurfte vorerst eine mögliche Unionsrechtswidrigkeit des § 7 Abs. 4 TMG, da über dessen Anwendung zunächst das OLG Düsseldorf zu entscheiden hat.

Der BGH hat in Bezug auf die Möglichkeit der Sperrmaßnahmen nicht zwischen dem offenen WLAN-Zugang und dem Tor-Exit-Knoten unterschieden. Möglicherweise sind die Maßstäbe der Unterbindung zukünftiger Missbrauchspotentiale für Betreiber solcher Netze strenger. Als letztes Glied in der Kette lassen sich nur diese zuverlässig über die IP-Adresse ermitteln. Abzuwarten bleibt daher die Entscheidung des Oberlandesgerichts, an das der BGH den Rechtsstreit zurückverwiesen hat. Für Tor-Nutzer selbst dürfte sich jedenfalls aber keine unmittelbare Änderung ergeben.

3. Entwicklung der Rechtslage

Die Abschaffung der Störerhaftung für Anbieter von WLAN-Zugängen war Gegenstand jahrelanger Diskussionen.[18] Bereits im Juli 2014 gab es erste Änderungsvorschläge, ein konkreter Entwurf zur Förderung öffentlicher Internetzugänge[19] wurde von Wirtschaftsminister Sigmar Gabriel im September 2015 vorgelegt. Nach einiger Kritik und Änderungen an diesem Entwurf trat das Zweite Gesetze zur Änderung des Telemediengesetzes (BGBl. I 2016 S. 1766) am 27.07.2016 in Kraft. Hierauf bezogen bestätigte der EuGH am 15.09.2016 zwar, dass ein WLAN-Betreiber für Rechtsverstöße Dritter nicht auf Schadensersatz haftet, allerdings wendet der EuGH das Haftungsprivileg nicht auf die Störerhaftung an. Auch stellte er klar, dass ein Passwortschutz, inklusive damit einhergehender Identitätsoffenlegung des Nutzers, zulässig sein kann.[20] Um den rechtssicheren Betrieb von offenen WLAN-Hotspots sicherstellen zu können, musste die Regierung daher nachbessern, weshalb am 13.10.2017 das Dritte Gesetz zur Änderung des Telemediengesetzes in Kraft trat.

4. Auswirkungen auf die Praxis: allem voran ein Sieg für die Digitalisierung

Insbesondere für den stationären Handel ist das Angebot eines offenen WLAN ein entscheidender Faktor zur Etablierung und Weiterentwicklung innovativer Kundenservices. Beispielsweise setzt die auf Kundenseite zunehmend an Zuspruch gewinnende mobile Bezahlung einen Internetzugang vom Geschäft aus voraus. Weil einem solchen Zugang nicht selten Hürden, wie etwa eine schlechte Mobilfunk-Netzqualität, entgegenstehen, lässt sich eine stabile Internetverbindung oftmals nur durch WLAN sicherstellen.

Ein für Handelsunternehmen entscheidender Faktor ist weiter, dass WLAN-Angebote nicht verpflichtend mit Passwörtern oder Registrierungen geschützt werden müssen, denn gerade zeitsparende Angebote – wie das bereits genannte Mobile Payment – würden hierdurch konterkariert. Unbenommen bleibt es den Betreibern selbstverständlich, ihr WLAN weiterhin nur mit Passwörtern oder nach vorheriger Registrierung zugänglich zu machen.

Unternehmen, die frei zugängliches WLAN anbieten, haben nun einerseits die notwendige Rechtssicherheit, nicht für mögliche rechtswidrigen Handlungen ihrer Kunden verantwortlich gemacht werden zu können. Andererseits bleibt aufgrund der weitgehenden Interpretation des Sperranspruchs von Rechteinhabern durch den BGH möglicherweise unklar, ob und unter welchen Voraussetzungen WLAN-Anbieter zur Verschlüsselung oder gar Sperrung gezwungen werden können. Abzuwarten ist insofern, wie nunmehr das im streitgegenständlichen Fall erneut zuständige OLG Düsseldorf entscheiden wird.

Nach Einschätzung des Handelsverband Deutschland (HDE) werde die Abschaffung der WLAN-Störerhaftung zu einem digitalen Innovationsschub im Einzelhandel führen.[21] Eine erwartete praktische Auswirkung der nunmehr verstärkten Rechtssicherheit sei die (noch) engere Verzahnung von Online-Angebote und stationären Geschäften, was wiederum mit einem Serviceplus auf Kundenseite einhergehen und die Digitalisierung des Einzelhandels sowie des öffentlichen Raums insgesamt vorantreiben werde. Potential hätte laut HDE insbesondere die sogenannte verlängerte Ladentheke, die es Kunden in Ergänzung zur Produktbegutachtung vor Ort ermögliche, zu-

17 *Sakowski*, BGH zur Störerhaftung – Abschaffung mit Hintertür, 26.07.2018, https://www.lto.de/recht/hintergruende/h/bgh-izr6417-stoererhaftung-wlan-hotspot-unterlassung-abmahnkosten-sperrmassnahmen/, zuletzt abgerufen am 30.08.2018.

18 Zum Gesetzgebungsverfahren sowie dem europäischen Hintergrund *Heckmann* in: Heckmann (Hrsg.), jurisOK-Internetrecht, 5. Aufl. 2017, Kap. 1 Rn. 2 ff., ebenso *Mantz*, GRUR 2017, 969, 970.

19 Vgl. hierzu beispielsweise *Bohsem*, Gesetzesentwurf für mehr öffentliche Internetzugänge, 17.09.2015, https://www.sueddeutsche.de/digital/digitale-agenda-gesetzesentwurf-fuer-mehr-oeffentliche-internetzugaenge-1.2650534, zuletzt abgerufen am 30.08.2018.

20 *Bundesministerium für Wirtschaft und Energie*, Mehr Rechtssicherheit bei WLAN.

21 *HDE*, Abschaffung der Störerhaftung: WLAN: Digitaler Innovationschub für den Handel, Pressemitteilungen 2017, https://www.einzelhandel.de/presse/pressearchiv/1327-pressemitteilungen-2017/9713-abschaffung-der-stoererhaftung-wlan-digitaler-innovationschub-fuer-den-handel, zuletzt abgerufen am 30.08.2018.

sätzliche Informationen sowie entsprechende Konfigurationsmöglichkeiten per Smartphone zu erhalten. Ferner lägen im Ausbau öffentlicher WLAN-Angebote auch große Chancen für die Innenstädte, denn neben dem Handel würden sich Gastronomie, Dienstleister aber auch Nahverkehrsunternehmen und die Verwaltung im Allgemeinen weiter digitalisieren.

5. Fazit und Ausblick: Technische Fragen bleiben offen

Auch wenn es sich auf den ersten Blick nur um einen Filesharing-Altfall handelt, so bestätigte der BGH mit diesem Grundsatzurteil die Vereinbarkeit des neuen TMG mit dem Europarecht. Zu verfolgen bleibt, wie möglicherweise verhängte Nutzungssperren konkret aussehen werden.

Jedenfalls aber bleibt die Hoffnung, dass mit der Gesetzesänderung der entscheidende Schritt hin zu mehr offenen WLAN-Hotspots getan ist, womit Deutschland im europaweiten Vergleich aufholen kann.

Lorenz

Der nächste Newsletter erscheint am 15. Dezember 2018. Sie finden den Newsletter und die Möglichkeit, sich an- und abzumelden, unter www.baywidi.de

Hinweise, Anregungen, Lob und Kritik sind herzlich willkommen. Schreiben Sie uns einfach unter baywidi@uni-passau.de

Impressum

Universität Passau
Innstraße 41
94032 Passau
Telefon: 0851/509-0
Telefax: 0851/509-1005
E-Mail: praesidentin@uni-passau.de
Internet: www.uni-passau.de
USt-Id-Nr.: DE 811193057

Organisation

Gemäß Art. 11 Abs. 1 BayHSchG ist die Universität Passau als Hochschule des Freistaates Bayern eine Körperschaft des öffentlichen Rechts und zugleich staatliche Einrichtung. Aufsichtsbehörde ist das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in München (Anschrift: Salvatorstraße 2, 80333 München).

Vertretung

Die Universität Passau wird von der Vorsitzenden des Leitungsgremiums, Präsidentin Prof. Dr. Carola Jungwirth, gesetzlich vertreten. Verantwortliche im Sinne des § 5 TMG (Telemediengesetz) ist die Präsidentin. Für namentlich oder mit einem gesonderten Impressum gekennzeichnete Beiträge liegt die Verantwortung bei den jeweiligen Autorinnen und Autoren.