forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

White Paper

TRACKING

Beschreibung und Bewertung neuer Methoden

White Paper

TRACKING

Beschreibung und Bewertung neuer Methoden

Autorinnen und Autoren:
Regina Ammicht Quinn[3], Andreas Baur[3]; Tamer Bile[2], Benjamin Bremert[6], Barbara Büttner[5], Olga Grigorjew[2], Thilo Hagendorff[3], Jessica Heesen[3], Nicole Krämer[8], Yannic Meier[8], Maxi Nebel[2], German Neubaum[8], Carsten Ochs[5], Alexander Roßnagel[2], Hervais Simo Fhom[7], Severin Weiler[4]

(1) Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe
(2) Universität Kassel, Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
(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
(8) Universität Duisburg-Essen, Sozialpsychologie

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

Inhalt

Zusammenfassung

Das Forum Privatheit veröffentlicht ein neues White Paper zum Thema „Tracking". Anlass dazu ist der Umstand, dass sich in den letzten Jahren neben dem klassischen HTTP-Cookie eine ganze Reihe an weiteren, ungleich invasiver und intransparenter agierenden Tracking-Verfahren etabliert haben. Das White Paper beschreibt die Technik hinter den Verfahren, klärt über Zulässigkeiten auf und zeigt anhand einer empirischen Erhebung, dass die Informiertheit unter den Nutzer(inne)n bezüglich neuartiger Tracking-Verfahren äußerst gering ist. Weiterhin bietet das White Paper Ausführungen über die wirtschaftliche Bedeutung des Trackings im Internet. Ebenfalls beleuchtet es aus soziologischer und philosophischer Perspektive den gesellschaftlichen Kontext sowie die gesellschaftliche Bedeutung des Trackings. Nicht zuletzt werden technische sowie rechtliche Empfehlungen zum Umgang mit Tracking gegeben. Insgesamt problematisiert das Forum Privatheit insbesondere den Umstand, dass bei der Benutzung internetfähiger Technologien ein Tracking des Nutzer/-innenverhaltens nahezu unumgänglich geworden ist. Ebenfalls als problematisch erachtet wird die Intransparenz des stattfindenden Trackings, die hohe Eingriffstiefe in die Privatheit sowie die Tatsache, dass Nutzer/-innen typischerweise keine geeigneten Optionen zur Vermeidung von Tracking zur Verfügung stehen.

1 Einführung

Tracking ist in modernen Informationsgesellschaften allgegenwärtig. Spätestens, seitdem durch eine EU-Regulierung auf vielen Webseiten das Cookie-Banner vorgeschrieben wurde, ist das Thema auch in der breiten Öffentlichkeit angekommen. Jedoch steckt hinter modernem Tracking viel mehr als die klassischen Browsercookies. In diesem Whitepaper sollen deshalb neuartige und weitgehend unbekannte Trackingmethoden und ihre Auswirkungen auf die Privatheit vorgestellt, besprochen und bewertet werden. Während Trackingtechnologien prinzipiell auch sehr viele Chancen für die Gesellschaft, Politik und Ökonomie mit sich bringen (beispielsweise die Übernahme von Koordinierungs-, Orientierung- als auch Ordnungsfunktionen), legt dieses Paper den Fokus auf die Beschreibung von Risiken bestimmter Formen des Trackings.

Das vorliegende Whitepaper entstand aus einer Zusammenarbeit zwischen Wissenschaftler(inne)n aus Rechtswissenschaft, Soziologie, Datenschutz, Informatik, Wirtschaftswissenschaft, Medienpsychologie und Ethik im Rahmen des vom Bundesministerium für Bildung und Forschung geförderten Projekts „Forum Privatheit". Die Zielsetzung des Whitepapers ist, das Phänomen des Trackings im Rahmen digitaler Technologien aus den verschiedenen disziplinären Perspektiven zu beleuchten und die Erkenntnisse in verständlicher und übersichtlicher Form zusammenzutragen.

Das Whitepaper ist in drei Teile aufgeteilt: Einen Beschreibungs-, einen Bewertungs- und einen Empfehlungs-Teil. Ersterer ist so gestaltet, dass mit einer generellen Beschreibung der Phänomene des Trackings begonnen wird, um anschließend einzelne thematische Schwerpunkte zu vertiefen. Zu diesen gehört die Einordnung des Trackings in einen größeren soziologischen Rahmen, die Erläuterung der technischen Hintergründe sowie die Beschreibung der ökonomischen Bedeutung des Trackings. Hinzu kommt eine empirische Studie, für welche unter anderem Erhebungen über die Informiertheit von Mediennutzer(inne)n hinsichtlich verschiedener Tracking-Technologien durchgeführt wurden. Ferner werden rechtliche Rahmensetzungen für das Tracking beschrieben, wobei im Besonderen auf das nahezu unbekannte Ultraschall-Tracking und dessen Zulässigkeit eingegangen wird. Den Abschluss des Whitepapers bilden Empfehlungen, welche sowohl technische Schutzmaßnahmen gegen Tracking-Verfahren betreffen als auch rechtliche Vorschläge zur Weiterentwicklung des Datenschutzrechts.

2 Beschreibung

2.1 Begriff

Mit dem Begriff ‚Tracking' wird im Allgemeinen die über einen längeren Zeitraum hinweg stattfindende Identifizierung und Nachverfolgung von Personen oder Dingen verstanden. Im engeren Sinne meint Tracking eine Form von Überwachung und soll im Rahmen dieses Whitepapers im Kontext digitaler Technologien beschrieben und analysiert werden. Dabei bezieht sich der Begriff ‚Tracking' klassischerweise auf Verfahren der Web-Analyse. Diese beschreibt die Erhebung von Daten über das Verhalten von Nutzer(inne)n beim Besuch von Webseiten. Dabei werden über das Cross-Domain-Tracking auch webseitenübergreifende Aufzeichnungen gemacht. Ferner werden über Datenbroker personenbezogene Profile, also aggregierte Daten über das Surfverhalten, aus verschiedenen Quellen miteinander kombiniert. Aufgrund der Sensibilität der Daten, welche unter anderem Hinweise über politische Einstellungen, persönliche Interessen, den sozioökonomischen Status etc. geben, sind Tracking-Verfahren häufig ein Problem für den Schutz der Privatheit und der informationellen Selbstbestimmung.

Das Ziel von Tracking-Verfahren insbesondere im Kontext der Web-Analyse besteht darin, dass Anbieter den Umgang von Nutzer(inne)n mit Webinhalten analysieren und optimieren können. Dies erfolgt in der Regel mit Hilfe von spezialisierten Drittanbietern wie etwa Google Analytics. So kann die Zahl von Seitenaufrufen, die Effektivität von Werbeinhalten oder die Zeit des Besuchs einzelner Seiten erhoben werden. Von Interesse sind diese Informationen insbesondere für die Werbeindustrie, deren Geschäftsmodell auf personalisierte Onlinewerbung fokussiert ist. Aber auch Scoring-Dienste, personalisierte Suchmaschinen, Empfehlungssysteme, Social-Media-Plattformen und viele weitere Anwendungen verfolgen ihre Nutzer/-innen. Dabei muss nicht zuletzt auch bedacht werden, dass Tracking nicht nur auf den Endgeräten und den darauf laufenden Anwendungen stattfindet, sondern auch, dass die Endgeräte als solche getrackt werden, beispielsweise in Supermärkten.

Das Tracking insbesondere im Kontext der Web-Analyse ist jedoch nicht ausschließlich negativ im Sinne einer Überwachungsmethode zu sehen. Es ist gleichzeitig an vielen Stellen die Voraussetzung für eine benutzerfreundliche Verwendung von Online-Plattformen und -Diensten. Ein Beispiel hierfür wäre etwa das Tracking beim Online-Shopping, bei welchem über den Besuch verschiedener Webseiten hinweg festgehalten wird, welche Gegenstände sich im Warenkorb befinden. Ferner ist das Tracking eine essentielle Voraussetzung dafür, dass Plattformen und Dienste personalisiert werden und individuelle, an die Nutzer/-innen angepasste Einstellungen gespeichert werden können. Jenseits der Vorteile des Trackings für einzelne Individuen können ferner nützliche Aspekte des Trackings für die Gemeinschaft erwähnt werden. So kann das Tracking des Verhaltens einer großen Anzahl an Nutzer(inne)n eines Webangebots beispielsweise zu einer Optimierung der Benutzeroberfläche verwendet werden.

2.2 Intransparenz

Das wohl bekannteste Verfahren zum Tracking von Internetnutzer/innen ist der Einsatz von Cookies.[1] Diese werden von Webseiten in Browsern abgelegt und protokollieren in Form von Textdateien den Besuch dieser Webseiten. Cookies waren und sind Gegenstand rechtlicher Auseinandersetzungen und Regelungen. Zahlreiche technische Verfahren zum Blocken oder zeitnahen Löschen von Cookies sind erhältlich. Das Bewusstsein und die Informiertheit um den Einsatz derselben dürfte nicht zuletzt aufgrund der in der EU durch die Datenschutzrichtlinie für elektronische Kommunikation vorge-

schriebenen Hinweismeldungen bei Nutzer(inne)n von Webangeboten relativ groß sein. Anders sieht dies bei Tracking-Methoden jenseits von klassischen Cookies aus, welche Gegenstand dieses Whitepapers sein sollen. So wurden in den letzten Jahren eine ganze Reihe neuer Tracking-Technologien entwickelt, über deren Einsatz die allermeisten Nutzer/-innen digitaler Medien nicht informiert sind, wie unter anderem die empirische Studie, welche für das vorliegende Whitepaper durchgeführt wurde, zeigt. Darüber hinaus gibt es zu den neueren Tracking-Technologien weder detaillierte datenschutzrechtliche Regelungen noch politische Aushandlungen hinsichtlich ihres hohen privatheitsverletzenden Potentials. Zu diesen neuen Tracking-Technologien gehören etwa der Einsatz von Ultraschall, das Tracking über biometrische Merkmale, nahezu unumgängliche softwarebasierte Tracking-Methoden, App- oder Smart-TV-Tracking, Tracking über das Internet der Dinge, Tracking per Session-Replay zur Aufzeichnung des gesamten Nutzerverhaltens auf einer Webseite und einiges mehr.

Gemeinsam ist allen diesen Methoden, dass sie möglichst effektiv und doch unauffällig funktionieren und gleichzeitig schlecht abzuwehren sind. Beim Tracking handelt es sich um eine spezielle Form von Überwachung, welche sich explizit dadurch kennzeichnet, dass sie auf der einen Seite sehr invasiv, auf der anderen Seite jedoch praktisch unbemerkt sowie immun gegen Abwehrmaßnahmen wie Löschen, Blockieren oder Vermeiden agieren kann. Tracking-Methoden sind zumeist so angelegt, dass für die Nutzer/-innen völlige Intransparenz herrscht, mit welchen Dritten die jeweils genutzten Plattformen oder Internetangebote Kontakt aufnehmen und personenbezogene Daten teilen.[2] Bei einer systematischen Untersuchung von einer Million populären Webseiten konnte herausgefunden werden, dass neunzig Prozent der Webseiten von Nutzer/-innen unbemerkt Daten an Drittanbieter weitergeben. Sechzig Prozent der Webseiten setzen Cookies von Drittanbietern bei Nutzer(inne)n. Und achtzig Prozent der Webseiten laden JavaScript-Code von externen Webseiten auf die Geräte der Nutzer/-innen.[3] Diese Zahlen belegen, dass bei der Nutzung von internetfähigen Geräten sich ‚im Rücken' der Nutzer/-innen unbemerkt ein riesiges Ökosystem an Tracking-Systemen gebildet hat, welches die Nutzung des Internets unweigerlich begleitet.

2.3 Trackingbeziehungen

Tracking wird typischerweise damit assoziiert, dass einzelne Unternehmen der IT-Branche oder auch mächtige Geheimdienste gegenüber einer Masse an Internetnutzer(inne)n überwachend agieren. Dabei sollten die Beziehungen des Trackings nicht zu einseitig betrachtet werden. In der Überwachungsforschung wurde durch Begriffe wie ‚social surveillance' oder ‚lateral surveillance' darauf hingewiesen, dass Überwachungsbeziehungen nicht nur institutioneller Natur sind, sondern sich auch zwischen einzelnen Bürger(inne)n entwickeln können.[4] Dasselbe gilt für den Bereich des Trackings. Die technischen Möglichkeiten zum Tracking sind letztlich für jedermann verfügbar. In Onlineshops können mit einfachen Mitteln beispielsweise GPS-Tracker erstanden werden, welche zur illegalen Nachverfolgung der Bewegungen anderer Personen eingesetzt werden können. Ein anderes Beispiel für das ‚social tracking' wäre etwa die Nachverfolgung von Kindern durch die Eltern.[5] Da Kinder bereits ab einem sehr jungen Alter, nicht anders als Erwachsene auch, Smartphones oder andere digitale Kommunikations- und Informationstechnologien nutzen, ist auch eine Verwendung jener Geräte zu Zwecken der Überwachung naheliegend. Dabei muss jedoch kritisch angemerkt werden, dass Kinder ebenso wie Erwachsene einen Anspruch auf den Schutz ihrer Privatheit besitzen. Dieser Anspruch wird jedoch durch Eltern, sofern sie etwa den Aufenthaltsort ihrer eigenen Kinder tracken, verletzt. Unabhängig von der Frage nach dem pädagogischen Sinn des Trackings von Kindern zeigt dieses Beispiel, dass Tracking immer allgegenwärtiger wird und nicht allein durch IT-Unternehmen durchgeführt wird. Dafür steht nicht zuletzt auch das freiwillige ‚Self-Tracking' oder ‚Lifelogging',[6] bei welchem Nutzer/-innen mit Hilfe digitaler Medien ihre sportlichen Aktivitäten, ihre Körperdaten, ihren Schlafrhythmus, ihre Ernährungsgewohnheiten und vieles mehr auf-

zeichnen und durch digitale Dienste und Plattformen verwalten lassen und auf denselben teilen. Die Erfassung dieser Angaben geht jedoch auch hier typischerweise einher mit der Weiterverwendung der Daten für kommerzielle Zwecke. Oder sie ermöglicht, wie am Beispiel des Fitnesstrackers Strava gezeigt wurde, sogar die Aufdeckung geheimer Militärbasen und anderer Stützpunkte.[7] Ein besonderes Problemfeld stellt das Tracking im Kontext der Benutzung von Geräten aus dem Internet der Dinge dar. Internetfähige Zahnbürsten, Sprachassistenzgeräte, smarte Autos, Module zur Heimautomation, Smart-TVs und andere kommunikationsfähige Geräte zeichnen sich typischerweise dadurch aus, dass sie nur ein minimales oder stark funktional limitiertes Interface aufweisen. Hier besteht für Nutzer/-innen kaum oder gar nicht mehr die Möglichkeit, überhaupt Maßnahmen zu ergreifen, das Tracking einzuschränken oder zu verhindern. Auf derartigen Endgeräten lassen sich weder Anti-Tracking Tools installieren, noch lässt sich überhaupt einsehen, wie ein mögliches Tracking erfolgt. Dies gilt auch für Technologien wie etwa Spielekonsolen, welche permanent ans Internet angebunden sind. Auch die darauf laufenden Spiele sind häufig überwachte Umgebungen, bei denen Spielerhandlungen nahezu lückenlos aufgezeichnet werden.[8] Ebenfalls ist das Tracking bei vernetzten Spielzeugen,[9] Sexspielzeugen[10] oder weiteren Geräten des „versteckten Internets“[11] problematisiert worden.

2.4 Privatheit und Anonymität

In modernen Gesellschaften ist es unter dem aktuellen Stand der Dinge quasi unmöglich, einem mehr oder minder umfänglichen Tracking des eigenen Verhaltens zu entkommen. Die intensive Nutzung von Smartphones, internetfähiger Unterhaltungselektronik, Wearables oder anderen Geräten aus dem Internet der Dinge oder klassischen Desktop-Computern, ergänzt durch weitere Überwachungstechnologien etwa im öffentlichen Raum, am Arbeitsplatz oder in Supermärkten, kombiniert durch die ausgesprochene Kreativität bei der Entwicklung neuer, invasiver und kaum auffindbarer Tracking-Methoden, lassen die Frage aufkommen, inwiefern ein ausreichender Schutz von Privatheit und informationeller Selbstbestimmung überhaupt noch gewährleistet werden kann. Tatsächlich ist es unter den derzeit gegebenen Bedingungen kaum noch möglich, anonym zu bleiben. Privatheit und Anonymität stellen jedoch wichtige Werte freiheitlicher, demokratisch verfasster Gesellschaften dar. Der Schutz des Privaten sichert Handlungsfreiheiten, die freie Entfaltung der Persönlichkeit sowie das Managen der eigenen Identität innerhalb verschiedener sozialer Kontexte.[12] Auch können die Grundrechte auf Privatheit und informationelle Selbstbestimmung einen Schutz bieten gegenüber staatlichen Übergriffen auf das persönliche Lebensumfeld. Anonymität wiederum ist eine Grundvoraussetzung dafür, dass Menschen in der Lage sind, etwa bei politischen Wahlen frei entscheiden oder auch kritische Meinungen frei äußern zu können. Ferner dient Anonymität dazu, bestimmte Eigenschaften oder soziale Identitäten gezielt aus verschiedenen sozialen Kontexten heraus zu halten.[13] Anonymität fungiert hier letztlich als Schutz vor Diskriminierung. In Umgebungen, in denen anonym kommuniziert werden kann, entfallen zudem Statusunterschiede. Es wird eine Kommunikation unter freien und gleichen Personen ermöglicht. Zwar soll nicht übersehen werden, dass Anonymität auch missbraucht werden kann, was an dieser Stelle jedoch nicht Thema sein soll. Wichtig ist, zu sehen, dass die Aufhebung von Privatheit und Anonymität durch tiefgreifende und allgegenwärtige Tracking-Verfahren nicht nur zu einer in der Literatur häufig als „context collapse“[14] bezeichneten Konvergenz eigentlich getrennter sozialer Kontexte führt. Genau dies widerspricht dem Grundrecht auf informationelle Selbstbestimmung, das die freie Entscheidung darüber schützt, welche Informationen aus unterschiedlichen sozialen Kontexten zusammengeführt werden soll.[15] Außerdem entsteht eine erhöhte Vulnerabilität gegenüber Unternehmen und Regierungen, welche Informationen über persönliche Eigenschaften, Interessen und Handlungen zur subtilen Kaufanregung, Manipulation oder gar Verhaltenssteuerung verwenden.[16]

2.5 Historischer und gesellschaftlicher Kontext

Tracking ist kein völlig neues Phänomen. Bereits mit dem Einzug der Moderne begann sich ein Trend zur Quantifizierung des Sozialen durchzusetzen – wenngleich es Bemühungen, Informationen über die Bevölkerung zu sammeln, beispielweise in Form von Volkszählungen, schon viel früher gab. Neben dem Einsatz als Kontrollinstrument zur Aufrechterhaltung der Herrschaftsordnung[17] dienen insbesondere die damit einhergehenden Erklärungs- und Objektivitätsversprechen rechnerischer Kennzahlen als Grundlage für zunehmende Maßnahmen hin zu immer mehr zahlenbasierten wirtschaftlichen oder politischen Entscheidungsprozessen.[18] Tracking kann aber auch als Bestandteil von Alltagspraktiken verstanden werden. Im Sinne eines Nachverfolgens von Spuren, die im Zuge sozialer Aktivitäten entstehen und gleichzeitig dazu beitragen, das Soziale zu bilden und aufrecht zu erhalten, kann es als soziokulturelle Grundoperation gelten.[19] Gerade in hochmodernen Verhältnissen, in denen man es oft mit nicht-persönlich bekannten Gegenübern zu tun hat – etwa in der Straßenbahn oder beim Bäcker – gerät das ‚Lesen informationeller Spuren' zur Daueraktivität, sofern die einander fremden sozialen Akteure permanent nach Anhaltspunkten Ausschau halten müssen, die Aufschluss darüber geben, mit wem man es zu tun hat, um darauf das eigene Verhalten abstimmen zu können.[20] Menschliche Vergesellschaftungsformen nutzen also seit langem Sichtbarmachungen, Darstellungen und Beschreibungen des Sozialen, um dieses dadurch zu bilden, zu ordnen und zu stabilisieren.[21]

In diesem Sinn hat Tracking Tradition, jedoch erhält es im Zuge der Neuzeit eine spezifische Qualität. Der Übergang von einer leibbezogenen Zeit- und Raumwahrnehmung hin zu einer abstrakten, „digitalen Raumzeit" ermöglicht erst die Vermessung der Welt.[22] Damit gemeint ist die mit steigender Granularität stattfindende Zerlegung und Unterteilung der Welt in beliebig kleine Messeinheiten,[23] die zu diesem Zwecke ihres ursprünglichen Kontextes enthoben werden, um sie physikalisch zu vermessen – man denke etwa an die Erfindung des Uhrwerks, wodurch eine abstrakte Zeitmessung möglich wurde – und zu archivieren. Raum und Zeit sowie die darin befindlichen, auch menschlichen Körper werden nun eindeutig lokalisierbar, eine „digitale Raumzeit" entsteht. Mit der zunehmenden Perfektionierung dieser Logik wird es immer schwieriger zu „vermeiden, in der Matrix Spuren zu hinterlassen. Im Prinzip ist das wohl möglich, aber es dürfte nicht ganz einfach sein."[24] Neuartige Trackingverfahren weisen noch eine weitere zeitgenössische Spezifizität auf: Während das Erzeugen, Darstellen und Sammeln von „sozialen Daten" schon lange als Teil der Produktion des Sozialen gelten kann, entstehen mit digitalen Plattformen Infrastrukturen des Sozialen, die von vornherein darauf angelegt sind, die vollzogenen Interaktionen aufzuzeichnen und so verfolgbar und analysierbar zu machen.[25] Dies galt für die Telefon- und Face-to-Face-Kommunikationen des 20. Jahrhunderts so nicht. Hier mussten eigens Abhörmaßnahmen ergriffen werden.

Aus der soziodigitalen Innovation ergibt sich für Vergesellschaftungsprozesse eine Transformation von ganz erheblicher Tragweite. Instanzen, die Wissen sowohl über das Soziale[26] als auch über die Subjekte[27] erzeugen, vervielfältigen sich massiv.[28] Immer mehr individuelle, ökonomische und staatliche Akteure erhalten Zugang zu großen „sozialen" Datensätzen. Diese Aktivitäten werden mit zunehmender wechselseitiger Durchdringung von Menschen und Technologien etwa durch Wearables, subkutane Sensortechnologien oder das Internet der Dinge maßgeblich gesteigert, gleichzeitig aber immer intransparenter. Die Konsequenzen sind schon jetzt weitreichend, denn die Verfahren zum Tracking stellen nicht nur Wissen über die Gesellschaft bereit, sie tragen auch aktiv zu ihrer Organisation und Gestaltung bei.[29] In diesem Sinne lässt sich das Tracking als Produktion von gesellschaftlichem und sozialem Wissen immer auch als Gesellschaftsproduktion verstehen, bei der etablierte soziokulturelle Legitimations- und Ordnungsmuster untergraben werden: wer oder was über wen oder was bei welcher Gelegenheit was wissen soll oder darf, wird unklar, weil verstärkt und tendenziell jede/-r über jede/-n alles Mögliche wissen kann. Letzteres bedeutet eben immer mehr als

bloßes Abbilden des Sozialen. Wissen über das Soziale birgt, zumindest in soziodigitalen Umgebungen, vielmehr immer auch die Möglichkeit der Intervention in Vergesellschaftungsprozesse.[30]

Verfahren des Trackings, wie sie im Rahmen von Internet-Anwendungen wie etwa Social-Media-Plattformen zum Einsatz kommen, stellen eine besonders „hochaufgelöste", granulare Vermessung und Aufzeichnung des Sozialen dar. Wurde zuletzt der soziale und historische Kontext des Trackings beleuchtet, so soll es im Folgenden speziell um die technische Funktionsweise moderner Tracking-Verfahren gehen.

2.6 Technik

Moderne Tracking-Techniken werden in der Regel entlang dreier Technologiekontexte zusammengefasst: Web, Mobile und Internet der Dinge.[31] Das Tracking im Web und über mobile Endgeräte fasst Ansätze zusammen, die eine Verfolgung der Aktivitäten eines/einer Internetnutzers/Internetnutzerin gegebenenfalls über mehrere Domains hinweg ermöglicht. Mit der wachsenden Allgegenwärtigkeit des Internets der Dinge entstehen allerdings neue Anreize, Nutzer/-innen vernetzter Technologien in vielen Lebensbereichen kontinuierlich zu orten und zu verfolgen. Im Fokus des folgenden Abschnitts sollen vorerst Online-Tracking-Mechanismen stehen.[32]

2.6.1 Tracking im Web

Beim Besuch einer Webseite werden für gewöhnlich neben dem Inhalt der aufgerufenen Webseite auch (dynamische) Inhaltselemente[33] von Drittparteien geladen und ausgeführt. Dies dient unter anderem der Einbindung zusätzlicher Dienste wie zum Beispiel sogenannten Social-Login- oder Sharing-Buttons digitaler sozialer Netzwerke. Doch neben scheinbar harmlosen Funktionalitäten nutzen viele Drittparteien ihre Einbindung in viele beliebte Webseiten, um kontinuierlich Informationen über die Nutzer/-innen zu sammeln, um detaillierte Nutzungsprofile zu erstellen und diese für Werbemaßnahmen einzusetzen. Ferner werden spezielle in Webseiten eingebettete Skripte genutzt, um Eingaben in Textfeldern mitzulesen, selbst wenn der/die Nutzer/-in die Daten gar nicht an die Webseite übermittelt hat.

Das Sammeln von Informationen über Nutzer/-innen im World Wide Web und deren Auswertung zum Zweck der Verfolgung und Überwachung des Nutzerverhaltens gegebenenfalls über mehrere Webseiten hinweg wird als Web-Tracking bezeichnet. Geschieht Web-Tracking über mehrere Seiten hinweg, spricht man vom Cross-Domain-Tracking. Die aus dem Web-Tracking resultierenden Nutzungsprofile beinhalten in der Regel sensible Informationen wie den Browserverlauf, Passwörter und den Standort. Diese Daten werden oft an Datenbroker übermittelt. So können beispielsweise Data-Management-Plattformen und andere Unternehmen diese Daten mit Daten aus Drittquellen anreichern und daraus Details über soziodemographische Merkmale, Interessen, Einkaufsgewohnheiten und weitere sensitive Attribute der Nutzer/-innen ableiten.[34]

Doch nicht nur Drittparteien überwachen und verfolgen unwissende Nutzer/-innen. Webseitenbetreiber erfassen ebenso Nutzerinformationen. Auch Suchmaschinen, E-Mail-Dienste, Cloudspeicherdienste, und weitere Content-Anbieter können Informationen über Inhalte, die Nutzer/-innen abrufen bzw. hochladen, sammeln und auswerten. In diesem Fall spricht man vom First-Party-Tracking, im Gegensatz zum zuvor beschriebenen Third-Party-Tracking.[35]

Für die Wiedererkennung der Nutzer/-innen bzw. deren Rechner im Kontext des Web-Trackings werden verschiedene Webtechnologien und Techniken zur Nutzeridentifikation entweder einzeln oder kombiniert verwendet. Abhängig von der Art und Weise, wie die Wiedererkennung vorbereitet und durchgeführt wird, lassen sich zwei Hauptklassen von Webtrackingtechniken unterscheiden[36] [37]: zustandsbehaftetes (engl. stateful) und zustandsloses (engl. stateless) Tracking. Beim zustandsbehafteten Tracking

Beschreibung

werden Informationen auf dem Rechner des/der Nutzers/Nutzerin gespeichert (z. B. Cookies) und später wieder ausgelesen, was dem Tracker ermöglicht, die Nutzer/-innen über mehrere Besuche der Seite und über mehrere Webseiten hinweg wiederzuerkennen. Beim zustandslosen Tracking werden Konfigurationsmerkmale des Browsers und des jeweils verwendeten Computers oder Mobilgeräts genutzt, um diese wiederzuerkennen.

Da herkömmliche Cookies leicht löschbar sind, zum Beispiel durch die Schließung des Browsers, wurden Ansätze entwickelt, die eine persistente Speicherung der Attribute aus herkömmlichen HTTP-Cookies ermöglichen. Die resultierenden Techniken sind zwar Cookies ähnlich, aber schwieriger für Browsernutzer/-innen zu löschen. Sie ermöglichen, zusammengetragene Information für den Server auch an anderen Speicherorten im Browser abzulegen, um den/die Nutzer/in weiterhin zuverlässig zu erkennen. In diesem Fall spricht man von Supercookies (auch Evercookies), welche für den/die Nutzer/-in aufgrund eingeschränkten Zugriffs auf Elemente schwieriger zu löschen sind. Supercookies nutzen mehrere dieser in-Browser-Methoden (vgl. [38]) und können, sollte versucht werden, den Inhalt einzelner (Super-)Cookies zu löschen, diese aus den übrig gebliebenen Speicherorten wiederherstellen.[39]

Bei sogenannten Flash-Cookies wird der Umstand ausgenutzt, dass das Flash-Plugin des Browsers die Speicherung von „local shared objects" erlaubt und diese kein Verfallsdatum haben. Flash-Cookies eignen sich optimal, um Nutzer zu tracken. Die gespeicherten Informationen sind zudem systemweit auch von anderen Browsern und auch im privaten Modus des Browsers abrufbar. Die Löschung von Flash-Cookies gestaltet sich oft schwierig, da nicht alle Browser die Möglichkeit besitzen, Flash-Cookies zu verwalten oder zu löschen.[40]

Eine weitere Methode zur persistenten Speicherung von Cookies sind E-Tags.[41] [42] E-Tags sind wie folgt zu verstehen: Ein Browser speichert Bilder zwischen, um diese bei einem wiederholten Seitenbesuch nicht erneut laden zu müssen. Damit der Cache des Browsers kohärent mit dem eventuell veränderten Bild auf dem Server bleibt, generiert der Browser die Prüfsumme des Bildes (ein Wert, mit dem die Integrität des Bildes geprüft werden kann) und schickt diese beim erneuten Besuch der Seite beim Laden des Bildes mit. Der Server kann nun – bei nicht übereinstimmendem Hash-Wert – mit einem neuen Bild oder – bei gleichem Hash – mit „unmodified" antworten. E-Tag-Cookies nutzen dies aus: Der/die Nutzer/-in lädt ein individuell erstelltes Bild beim ersten Besuch der Webseite. Der Server nimmt keine Änderung des Bildes vor oder wenn, dann nur minimal. Bei erneuten Seitenbesuchen überträgt der/die Nutzer/-in die Prüfsumme des Bildes, woran der Server ihn wiedererkennt.[43] [44]

Eine weitere Form des Trackings geschieht über sogenannte Social Widgets. Möchten Nutzer/-innen Inhalte von anderen Internetseiten teilen oder „liken", dann bieten Social-Media-Plattformen hierfür Komfortfunktionen an. Hierfür müssen Inhaber beliebiger Webseiten einen „Gefällt mir"- oder „Teilen"-Button auf ihrer Seite einfügen. Hierbei handelt es sich um ein Social Widget, welches auch als „social plugin" bezeichnet wird. Klickt ein Anwender auf ein solches Widget, wird die Seite, auf der das Widget vorhanden ist, auf die Pinnwand des Anwenders kopiert. Somit wird das Teilen der Internetseite vereinfacht. Umgekehrt wird jedoch Tracking ermöglicht. Ist ein/-e Anwender/-in in einem digitalen sozialen Netzwerk eingeloggt, wird anschließend ein Cookie mit einer eindeutigen Identifikationsnummer auf dem Rechner erstellt. Da das Widget den Server des sozialen Netzwerkes kontaktiert, weiß dieser, auf welcher Seite sich der Anwender derzeit befindet. Dies geschieht durch die reine Anwesenheit des Widgets und ohne, dass es verwendet werden muss. Dadurch ist das Tracken eines/einer Anwenders/Anwenderin über alle Internetseiten, welche Social Widgets benutzen, möglich.

Neben den erwähnten zustandsbehafteten Tracking-Verfahren basiert das zustandslose Tracking darauf, möglichst viele Details über den/die Nutzer/-in und das genutzte System zu sammeln, um ihn bei einem späteren Besuch wiederzuerkennen. Dabei ist man

nicht darauf angewiesen, Informationen wie Cookies, die gelöscht werden könnten, auf dem persönlichen Computer zu hinterlegen. Stattdessen werden unterschiedliche Hardware-, Netzwerk- und Software-Charakteristiken des Geräts ermittelt und zu einem eindeutigen Gesamtmerkmal, einem „Fingerabdruck", aggregiert (vgl. [45] [46] [47]). Gerätecharakteristiken werden in der Regel über versteckte Skripte, kaum sichtbare Bilder und schlecht geschützte Programmierschnittstellen erfasst und an Tracker-Dienste übermittelt.

Die Electronic Frontier Foundation (EFF) stellte mit Hilfe der Seite www.panopticlick.eff.org, auf welcher die Eindeutigkeit des eigenen Browserfingerabdrucks getestet werden kann, fest, dass 94,2 % der Browser, die Flash oder Java aktiviertet haben, eindeutig identifizierbar sind und dass selbst veränderte Fingerabdrücke in 99,1 % der Fälle dem vorherigen Fingerabdruck richtig zugeordnet werden konnten.[48] Weitere Untersuchungen durch Acar et al.[49] [50] und zuletzt durch Englehardt und Narayanan[51] weisen auf die weite Verbreitung ziemlich ausgefeilter Fingerprinting-Techniken auf zahlreichen prominenten Webseiten hin. Beispiele derartig ausgefeilter Fingerprinting-Techniken sind Canvas Font Fingerprinting, Canvas Fingerprinting, WebRTC-based Fingerprinting, Audio Fingerprinting, Battery API Fingerprinting und Session-Replay Skripe.

Das Canvas Font Fingerprinting beispielsweise nutzt den Umstand aus, dass sich über JavaScript und Flash eine Liste von Schriftarten auslesen lässt, welche auf einem Computer installiert sind und damit dem Internetbrowser zur Verfügung stehen. Diese Liste variiert je nach installierter Software auf einem Computer, da Programme ihre eigenen Schriftarten mitbringen können. Diese Liste kann für das Canvas Font Fingerprinting verwendet werden, bei welchem Anwender/-innen anhand dieser Liste identifiziert werden.[52] Dadurch, dass nur ein Teil der Software eigene Schriftarten installiert, besteht die Wahrscheinlichkeit, dass andere Anwender/-innen eine identische Liste von Schriftarten auf ihrem Computer besitzen, was die Ergebnisse des schriftbasierten Fingerprintings verfälscht. Nichtsdestotrotz schränken sie den Kreis der möglichen Individuen enorm ein.

Eine weitere Tracking-Methode, welche hier beispielhaft erwähnt sein soll, ist das Fingerprinting über die Akku-Schnittstelle. Internetseiten bzw. Dritte können den aktuellen Akkustand und die Be- und Endladegeschwindigkeit eines verwendeten Akkus über die Akku-Schnittstelle abrufen. Je nach Alter, Kapazität und Nutzung eines Akkus sind diese Werte auch bei gleichen Akkus verschieden. Basierend darauf lassen sich einzelne Anwender/-innen identifizieren.[53] Voraussetzung für diese Trackingmethode ist das Vorhandensein eines Akkus, was auf Laptops und mobile Endgeräte zutrifft, jedoch nicht auf Desktop-Computer. Entsprechend ist diese Methode nur eingeschränkt nutzbar. Um das Tracking einzuschränken, haben einige Browserhersteller den Zugriff von Webseiten auf die Akku-Schnittstelle unterbunden [vgl. z. B.[54]].

Session-Replay-Skripte, ein weiteres zustandsloses Tracking-Verfahren, stellen ebenfalls eine ausgesprochene Bedrohung für die informationelle Privatheit der Nutzer/-innen dar. Session-Replay-Skripte werden von Drittanbietern bereitgestellt und können vom Seitenbetreiber in die Webseite eingebunden werden. Wird dies gemacht, können alle Nutzer/-inneneingaben wie Tastatur- und Mausaktivitäten an Drittserver übertragen werden. So kann zum Zweck der Besucher- oder Fehleranalyse der Seitenbesuch rekonstruiert werden – daher der Begriff „Session-Replay" („Sitzungswiederholung"). Ein Webinterface erlaubt es dem Seitenbetreiber dadurch, Verhaltensmuster der Seitennutzer/-innen zu erkennen. Der Betreiber sieht dabei genau, was der/die Internetnutzer/-in in seinem Browserfenster sieht.

2.6.2 Tracking bei Mobilgeräten

Mobile Endgeräte wie etwa Smartphones bieten diverse Möglichkeiten, private Informationen abzugreifen und an Dritte weiterzugeben. Sie ermöglichen damit auch Tracking. Dazu zählt etwa das biometrische Tracking. Bei diesem werden unter anderem

Beschreibung

Wischgesten, welche Nutzer/-innen in einer App ausführen, die Art der Tastaturbedienung, die Dicke des Daumens etc. aufgezeichnet und als biometrische Merkmale den jeweiligen Nutzer/-innen zugeordnet. Firmen wie BioCatch setzen das biometrische Tracking ein, um etwa Betrugsversuche beim Online-Banking abzuwehren. Denkbar ist allerdings auch, dass das biometrische Tracking für kommerzielle Zwecke jenseits der IT-Sicherheit verwendet wird.

Neben dem biometrischen Tracking gibt es diverse weitere Tracking-Verfahren, welche mit mobilen Apps verbunden sind. Für viele Funktionen in Apps werden Zusatzbibliotheken verwendet, welche es ermöglichen, Details über die App-Nutzer/-in zu erfassen. Bei einem Versuchsaufbau, in welchem 20 Teilnehmer ihr Smartphone für drei Wochen beim alltäglichen Gebrauch untersuchen ließen, fanden die Forscher heraus, dass 75 % der genutzten Apps den Nutzer getrackt haben. Werbe- und Tracking-Libraries eines Drittanbieters konnten in 57 % der Apps nachgewiesen werden.

Neben dem Tracking des Nutzerverhaltens innerhalb von Apps und anderer Software auf Mobilgeräten existiert die Möglichkeit des räumlichen Trackings von Mobilgeräten an sich. Mobilgeräte haben die Möglichkeit, via Triangulation im Mobilfunknetz[55] und in lokalen Funknetzen[56] ihre Position zu bestimmen. Da solch ein mobiles Endgerät ein täglicher Begleiter ist, lassen sich somit Bewegungs- und damit Interessenprofile der Anwender erstellen. [57] [58] [59] [60] [61] Diese Möglichkeiten werden durch eine zusätzliche Interpretation umfangreicher Sensordaten ergänzt. Neben herkömmlichen Mikrofonen und Kameras werden in Mobilgeräten zahlreiche andere Sensoren verbaut, darunter Beschleunigungs-, Gyroskop-, Ortungs-, Helligkeits-, Abstands-, Herzschlag-, Fingerabdruck-, Gesichtserkennungs-, Iris-Scanner- oder Luftdrucksensoren. Diese Sensoren ermöglichen viele neue Anwendungsmöglichkeiten, können allerdings auch genutzt werden, um einen Fingerabdruck des Gerätes zu generieren. Letzterer kann anschließend verwendet werden, um wortwörtlich jeden Schritt des/der Nutzers/Nutzerin offline und online zu überwachen.

Ein weiterer Aspekt des Trackings ist das Cross-Device-Tracking. Da Tracker sowohl auf Desktop-Computern als auch auf mobilen Systemen eingesetzt werden, wird erforscht, wie die gewonnenen Informationen zur besseren Nutzer/-innenerkennung und -verfolgung kombiniert werden können. Laut einer Google-Umfrage aus dem Jahr 2012 benutzen 98 % der Befragten mehrere Geräte am selben Tag. 90 % starten eine Aktivität an einem Gerät und führen diese auf einem anderen fort.[62] Es ist also für Tracker interessant, den/die Nutzer/in über verschiedene Geräte hinweg zu verfolgen. Man unterscheidet zwischen deterministischen und probabilistischen Methoden des Cross-Device-Trackings. [63] [64] [65] [66] Der deterministische Ansatz erkennt den/die Nutzer/in verschiedener Geräte dadurch, dass dieser sich auf den jeweiligen Geräten mit demselben Account oder derselben E-Mail-Adresse einloggt. Dabei erhöhen Social Widgets und ähnliche Dienste, die zur Einbettung in andere Seiten zur Verfügung stehen, den Wirkungsbereich der deterministischen Tracker. Der eingebettete Code erkennt den/die eingeloggte/-n Nutzer/-in wieder und meldet dem Server den Besuch auf der eingebetteten Seite. Eine Interaktion mit dem Widget ist hierzu nicht nötig. Doch auch ohne direkte Einbindung eines Trackers kann eine Webseite beispielsweise die E-Mail-Adresse eines/einer eingeloggten Nutzers/Nutzerin an Tracker weitergeben. Besucht ein/e Nutzer/in zum Beispiel mit dem Desktop-Rechner eine Seite, auf welcher er/sie eingeloggt ist, und mit dem Smartphone eine andere Seite, auf welcher er/sie sich mit derselben E-Mail-Adresse einloggt, und geben beide Seiten diese Information an denselben Cross-Device-Tracker weiter, kann dieser die über beide Geräte gesammelten Informationen miteinander verknüpfen.[67]

Beim probalistischen Cross-Device-Tracking hingegen wird versucht, ohne einen eindeutigen Login verschiedene Geräte einem/einer Nutzer/-in anhand anderer gesammelter Merkmale zuzuordnen. Hierzu müssen zunächst die einzelnen Geräte durch herkömmliches Tracking individuell wiedererkannt werden. Anschließend können die gewonnenen Informationen miteinander verglichen werden, um Geräte, die mit einer

hohen Wahrscheinlichkeit dem/der gleichen Nutzer/-in gehören, miteinander zu verknüpfen. IP-Adressen sind hierbei ein wichtiges Merkmal. Nutzen zwei Geräte die gleiche IP-Adresse für Webanfragen, befinden sie sich im selben Netzwerk hinter einem gemeinsamen Router. Standortdaten können ebenfalls in diese Betrachtung miteinbezogen werden. Um die Geräte noch besser miteinander verknüpfen zu können, können weitere Details, wie etwa Statistiken über häufig besuchte Seiten, berücksichtig werden.[68]

Eine weitere Option, Nutzer/-innen über mehrere Geräte hinweg verfolgen zu können, ist die Verwendung sogenannter „Ultrasonic Side Channels" (Ultraschall-Seitenkanäle).[69] [70] Hierbei sendet und empfängt ein Gerät kaum oder nicht wahrnehmbare Töne im Ultraschall-Frequenzbereich von 20 kHz. Diese Töne werden zur Datenübertragung für das Tracking verwendet. Über die Töne werden unterschiedliche Geräte identifiziert, verlinkt und einem Nutzer eindeutig zugeordnet. Ultraschall liegt mit 20kHz knapp oberhalb der Reichweite des Hörvermögens einer erwachsenen Person, ist jedoch für Lautsprecher und Mikrofone in Smartphones erfassbar.

Diese Form des Trackings ermöglicht neuartige Anwendungen, darunter geräteübergreifendes Tracking, die Verbindung verschiedener Endgeräte eines Nutzers und Tracking innerhalb von Räumen (vgl. [71] [72] [73]). Beim geräteübergreifenden Tracking werden Ultraschallsignale in Webseiten oder Audiospuren anderer Medien wie TV und Radio eingebettet und mit Hilfe entsprechender Zusatzbibliotheken in Apps wiedererkannt. Hierdurch können Geräte untereinander verlinkt werden. Auf Basis der damit aufgebauten Verknüpfungen lassen sich Nutzer/-innen charakterisieren und ihre Medieninteressen analysieren. Ultraschall-Tracking kann ebenfalls zur Verbindung verschiedener Geräte eines/einer Nutzers/Nutzerin genutzt werden.[74] Dieses Cross-Device-Tracking mittels Ultraschallsignalen bildet ein wesentliches Instrument für Analytics-Firmen wie „Silverpush" oder „audible magic". Laut einer jüngst veröffentlichten Studie von Arp et al.[75] konnte die Silverpush-Zusatzbibliothek in 234 Android-Apps mit 10.000 oder mehr Downloads nachgewiesen werden. Setzt der Cross-Device-Tracker zusätzlich einen Cookie beim Anzeigen oder dem Aufbau der Werbung auf einem Gerät ein, können nun mit hoher Wahrscheinlichkeit alle Geräte, die das Ultraschallsignal empfangen, diesem Cookie zugeordnet werde. Die Federal Trade Commission (FTC) der USA beobachtet diese Technologieentwicklung mit Sorge und rief kürzlich App-Entwickler dazu auf, auf Ultraschall-Tracking in ihren Apps zu verzichten.[76] Ultraschallsignale werden ebenfalls verstärkt für das Tracking in Gebäuden wie etwa in Einkaufsläden eingesetzt – mit unter Umständen schwerwiegenden Folgen für die informationelle Selbstbestimmung.[77] [78]

2.7 Ökonomie

Durch den Einsatz von einem oder mehreren der oben beschriebenen Tracking-Verfahren ist es für Unternehmen möglich, ein sehr differenziertes Bild ihrer Kund(inn)en zu erlangen. Die durch Tracking gesammelten Informationen werden hauptsächlich im Online-Marketing genutzt, das mittlerweile fest in die tägliche Praxis vieler Unternehmen integriert ist. Allein von 2011 bis 2016 stiegen die Bruttowerbeaufwendungen im Online-Marketing unter deutschen Handelsunternehmen um jährlich 9,3 % auf 14 % an.[79] Auf zwei ökonomisch bedeutsame Beispiele für Verwendungsfelder dieser Daten soll in diesem Abschnitt eingegangen werden: die Personalisierung von Werbung sowie Preisdiskriminierung.

Personalisierte Online-Werbung, das sogenannte „behavioral targeting", ist ein wichtiger Bestandteil des Online-Marketing-Mix. Dabei ist es gängige Praxis, Nutzer/-innengruppen aus durch Tracking gewonnenen Daten zu generieren, welche dann über ein Auktionssystem vermarktet werden.[80] Werbeinteressierte (z. B. Webseitenbetreiber) können hier darauf bieten, einer bestimmten Kundengruppe die eigene Werbung schalten zu dürfen. Durch das behavioral targeting können werbende Unterneh-

men zielgerichtet Kund(inn)engruppen ansprechen und somit die Effektivität der bereitgestellten Werbebotschaften erhöhen. Idealerweise sinkt dabei für Kund(inn)en gleichzeitig der mit der Suche nach einem geeigneten Produkt verbundene Aufwand. Betreiber einer Webseite erschließen sich über den Verkauf der Werbeflächen wiederum eine wichtige Erlösquelle. Durch Tracking ist es Anbietern also prinzipiell möglich, die am besten passende Zielgruppe für einzelne Produkte zu identifizieren und somit ihre Produkte effektiver zu vermarkten. Trotz teils widersprüchlicher Forschungsergebnisse zu den Effekten von personalisierter Werbung[81] finden diese Techniken in der Praxis sehr häufig Anwendung. 2014 teilten bereits 90 % der 500 beliebtesten Webseiten weltweit die Daten Ihrer Nutzer/-innen mit Drittanbietern[82], primär um damit zusätzliche Erlösquellen zu generieren. Diese Praktiken haben jedoch ihren Preis, denn der Vertrieb der Daten der Webseitenbesucher erfolgt mitunter ohne deren Einverständnis oder wird ohne ihr Wissen gesammelt.

Neben personalisierter Werbung wird durch Tracking auch die sog. Preisdiskriminierung immer wichtiger. Webseitenbetreiber, welche mittels Trackingverfahren und durch den Handel mit Nutzer/-innendaten große Datenmengen sammeln, können diese auch dazu nutzen, ihre Preise optimal an die Zahlungsbereitschaft des/der Nutzer/in anzupassen. Mithilfe der gesammelten Daten und durch den Abgleich mit den Daten anderer Nutzer/innen lassen sich statistische Vorhersagen zur Zahlungsbereitschaft der Nutzer/innen treffen, die deutlich präziser sind als bisherige Verfahren.[83] Neben den durch Tracking gewonnen Daten werden auch anderweitig erhobene, teilweise öffentlich zugängliche Daten im Zuge von Big-Data-Analysen zur Preisdiskriminierung genutzt.[84] Aus der Brille der neoklassischen Wirtschaftstheorie ist Preisdiskriminierung für Unternehmen grundsätzlich sinnvoll, da der Anbieter durch die individuellen Reservationspreise seine Margen über seine gesamte Kundenbasis hinweg optimieren kann.[85] Für Kunden kann sich Preisdiskriminierung aber nur dann positiv auswirken, sollten sie für die Preisgabe von persönlichen Informationen belohnt werden.[86] Rayna et al. (2015) zeigen modellhaft, dass sich durch eine Vergütung von persönlichen Informationen die gesamtwirtschaftliche Situation verbessern kann. Abseits der Theorie zeigen jedoch Beispiele wie das von Amazon aus dem Jahr 2000, dass kulturelle Normen einen starken Einfluss auf dieses unternehmerische Instrument haben. Als bekannt wurde, dass Amazon individuelle Preisdiskriminierung in den USA getestet hatte, entschuldigte sich der CEO öffentlich und ließ knapp 7000 Kund(inn)en entschädigen. Insgesamt lässt sich deshalb sagen, dass Tracking eine hohe ökonomische Bedeutung für Webseitenbetreiber und Drittanbieter hat. Jedoch kann es ökonomisch nachteilig für Nutzer/-innen sein: einerseits aufgrund der unentgeltlichen Verwendung ihrer Nutzerdaten und andererseits auch direkt durch eine vom Anbieter optimierte Preissetzung.

Anhand der personalisierten Onlinewerbung als auch der Preisdiskriminierung lässt sich bereits ablesen, dass das Tracking mit zahlreichen Risiken verbunden ist, welche sich negativ auf die Nutzer/-innen digitaler Medien auswirken können. Im folgenden Abschnitt sollen daher im Rahmen einer Bewertung von Tracking-Verfahren spezifische Risiken benannt werden. Teil der Bewertung ist ferner eine empirische Erhebung über die Informiertheit von Nutzer/-innen bezüglich verschiedener Tracking-Verfahren sowie eine rechtswissenschaftliche Einordnung der Zulässigkeit von Methoden des Trackings.

3
Bewertung

3.1 Risiken

Es wurde bereits deutlich, dass das Tracking mit zahlreichen Risiken in Hinsicht auf den Schutz personenbezogener Daten verbunden ist. Aber auch darüber hinaus ist Tracking mit vielen Risiken und Missbrauchsmöglichkeiten verbunden. Durch die umfangreiche Nachverfolgung des Mediennutzungsverhaltens sowie die Sammlung personenbezogener Informationen und die daran anschließende Profilbildung wird ein ‚social sorting' ermöglicht.[87] Hierbei werden Personen zum Beispiel in verschiedene Risiko-, Reputations-, Status-, Einkommens-, Verdachtsgruppen eingeordnet. Dabei kann es zu ungerechtfertigter Diskriminierung kommen, etwa hinsichtlich der Vergabe von Arbeitsstellen, Versicherungstarifen, Krediten oder in Bezug auf andere Entscheidungen.[88] Ferner wird das Tracking problematisiert aufgrund der Gefahr der Verbindung von digitalen Datenspuren mit ‚echten' Personen. Eine derartige Identifizierung von Personen führt zu einer stärkeren Verschmelzung von Online- und Offline-Tätigkeiten. Ein weiterer Aspekt ist, dass Tracking-Verfahren eines der herausragenden Symptome der Kommerzialisierung des Internets darstellen. Ökonomische Logiken bestimmen weite Teile von digitalen Medien und Plattformen, mit den entsprechenden Konsequenzen für die Offenheit, Transparenz oder Neutralität jener Medien und Plattformen. Nicht zuletzt kann Tracking auf grundlegende Weise mit der Verletzung der informationellen Selbstbestimmung in Verbindung gebracht werden. Die auf Seiten der Nutzer/-innen fehlende Kontrolle über die Verbreitung und Verwendung personenbezogener Informationen steht in fundamentalem Widerspruch zu den Normen der informationellen Selbstbestimmung und dem Schutz der Privatheit.

Gerade letzterer Aspekt soll an dieser Stelle von besonderer Bedeutung sein. Wie oben bereits erwähnt, sind die Risiken und Gefahren klassischer Tracking-Verfahren auch und gerade hinsichtlich von Fragen des Schutzes der Privatheit vielerorts bereits hinreichend beschrieben. Weniger Aufmerksamkeit wurde bislang jedoch dem Umstand getragen, dass durch neue Technologien sowie durch die immer tiefgreifendere Durchsetzung der persönlichen Lebenswelt mit digitalen Medien eine neue Qualität und eine neue Dimension des Trackings sowie der damit verbundenen Verletzungen von Privatheit und Selbstbestimmung entstanden ist. Waren klassische Tracking-Verfahren, welche etwa über HTTP-Cookies operieren, anfangs noch leicht zu detektieren, so sind nun neue Dimensionen von Tracking-Methoden vorzufinden, denen kaum auszuweichen ist und welche gleichzeitig mit einer extremen Immunität gegen Abwehr- und Schutzmaßnahmen ausgestattet sind. Dabei ist besonders der Umstand als problematisch zu sehen, dass eine erfolgreiche Anwendung von Abwehr- oder Schutzmaßnahmen in der Regel mit einer Einschränkung der Funktionalität von Webangeboten einhergeht. So stehen die Nutzer/-innen vor der Wahl, ihr Mediennutzungsverhalten entweder in umfänglicher Weise technisch nachverfolgen zu lassen, um bestimmte Dienste und Plattformen nutzen zu können. Oder sie versuchen, sich gegen bestimmte Methoden des Trackings zu schützen, müssen dann jedoch auf Inhalte oder Funktionen jener Dienste und Plattformen verzichten. Umgekehrt ist zu sehen, dass viele Dienste und Plattformen gar nicht anders kostenlos angeboten werden könnten, wenn die Nutzer/-innen nicht mit ihren Daten zahlen würden.[89] Dennoch könnten genau diese Mechanismen transparenter gemacht werden, als dies derzeit der Fall ist.

3.2 Verdinglichung

Self-Tracking ist immer ein Stück weit verbunden mit einer Verdinglichung des eigenen Körpers, also seiner Objektivierung nach einer bestimmten (quantifizierbaren) Maßga-

be. Ebenso kann das umfangreiche Tracking im Kontext der Nutzung digitaler Medien als eine Verdinglichung von Personen beschrieben werden, d. h. die jeweilige Person erhält einen bestimmten „Preis“. Das Mediennutzungsverhalten wird, sobald es dem Tracking unterworfen wird, letztlich als etwas gesehen, aus dem ökonomischer Nutzen gezogen werden muss. Tracking zielt dabei, wie beschrieben, insbesondere auf eine Präzisierung personenbezogener Werbung, sodass Kaufanreize gezielter gesetzt werden können. Die Nutzung des Internets oder internetfähiger Geräte wird somit zu einem bloßen Vehikel zur Setzung von Anreizen zum Konsum von Dienstleistungen oder Produkten oder auch zur Befürwortung oder Wahl einer politischen Partei. Hinzu kommt, dass dies in einem Rahmen geschieht, welcher bewusst auf Intransparenz setzt und die Uninformiertheit der Nutzer/-innen ausnutzt. Den meisten Internetnutzer/-innen ist bewusst, dass personenbezogene Informationen, welche etwa im Zuge des Onlineshoppings in eine entsprechende Maske eingetragen werden, gespeichert und weiterverwendet werden. Darüber hinaus werden aber neben dieser Art der Informationsübertragung diverse weitere Kanäle und Analysemethoden zum Tracking genutzt. Dies geht, wie ebenfalls oben beschrieben, beispielsweise von einem Tracking der Mausbewegungen über die Aufzeichnung darüber, wie lange bestimmte Elemente angesehen werden, bis hin zum unhörbaren Versenden von Ultraschallsignalen oder dem Tracking von biometrischen Eigenschaften etwa bei der Aufzeichnung der Wischgesten auf einem berührungssensitiven Bildschirm. Dass derartige Methoden zum Einsatz kommen, zeigt, dass eine gezielte Hintergehung von Nutzer/-innen beabsichtigt wird. Dies setzt sich auch darin fort, dass ein von Seiten der Nutzer/-innen ausgehendes Löschgesuch gegenüber trackenden Institutionen gar nicht sinnvoll ist, da nur bedingt Kenntnisse darüber vorhanden sind, dass und wie überhaupt das Tracking erfolgt, welche Informationen dabei erhoben werden und wie diese ausgewertet werden. Wie weit die Kenntnisse über verschiedene Tracking-Verfahren dabei reichen und wie diese seitens der Nutzer/innen bewertet werden, soll im Folgenden genauer beleuchtet werden.

3.3 Kenntnisse und Bewertungen der Nutzer/-innen

Um die aktuelle Informiertheit der Nutzer/-innen zu Tracking-Verfahren zu erfassen, wurde im November 2017 eine Online-Befragung mit 441 Personen (nicht-repräsentative deutschsprachige Stichprobe) zu fünf ausgewählten Tracking-Verfahren durchgeführt. Dabei war von Interesse, wie bekannt einige neuartige Tracking-Verfahren bei Nutzer/-innen des Internets, mobiler Endgeräte sowie von Videospielen sind und welche Einstellungen deutsche Nutzer/innen gegenüber diesen Verfahren haben. Die Stichprobe setzte sich wie folgt zusammen: 50,3 % Frauen, 48,5 % Männer, 1,1 % keine Angabe. Das durchschnittliche Alter der Befragten betrug 31,81 Jahre (12-82; *SD* = 12,77) und der Großteil der Befragten waren Studierende (45,4 %) und Erwerbstätige (40,1 %). Die fünf ausgewählten Tracking-Verfahren deckten die Bereiche Tracking mithilfe des Browsers (Canvas Fingerprinting und Evercookies), Tracking mithilfe von Ultraschall (uBeacons), biometrisches Tracking (Touchscreen Wischbewegungen) und Tracking in Videospielen ab. Die jeweiligen Tracking-Verfahren wurden den Teilnehmenden durch kurze Beschreibungen über Funktionsweise und Einsatz präsentiert. Auf der Grundlage dieser Beschreibungen sollten die Befragten angeben, ob ihnen das Tracking-Verfahren bereits vor der Befragung bekannt war oder nicht. Zusätzlich beantworteten die Teilnehmenden eine Reihe von Aussagen zu jedem Verfahren. Wie die Auswertung der Daten ergab, kannte die Mehrheit der Befragten die fünf Verfahren nicht, wobei die Bekanntheit zwischen den Technologien stark schwankte (siehe Abbildung 1). Tracking in Videospielen war 186 (42,2 %) Teilnehmenden bekannt, Evercookies kannten 180 Personen (40,8 %), biometrisches Tracking (Touchscreen Wischbewegungen) kannten 147 Befragte (33,3 %), Canvas Fingerprinting war 104 Teilnehmenden (23,6 %) ein Begriff und das Schlusslicht bildete Tracking mithilfe von Ultraschall (uBeacons) mit gerade einmal 60 positiven Antworten (13,6 %). Zwei erste Erkenntnisse lassen sich aus diesen Daten ableiten. Zum einen

zeigt sich, dass die Bekanntheit der Verfahren stark schwankt, was darauf hindeutet, dass sich Informationen zu den Verfahren unterschiedlich schnell verbreiten. Zum anderen wird deutlich, dass nur wenige Menschen überhaupt von diesen Verfahren gehört haben. Denn obwohl die Bekanntheit unterschiedlich ist, liegt sie dennoch immer unter 50 % und somit sind alle Verfahren weniger als der Hälfte – teils weniger als einem Viertel – der Befragten bekannt.

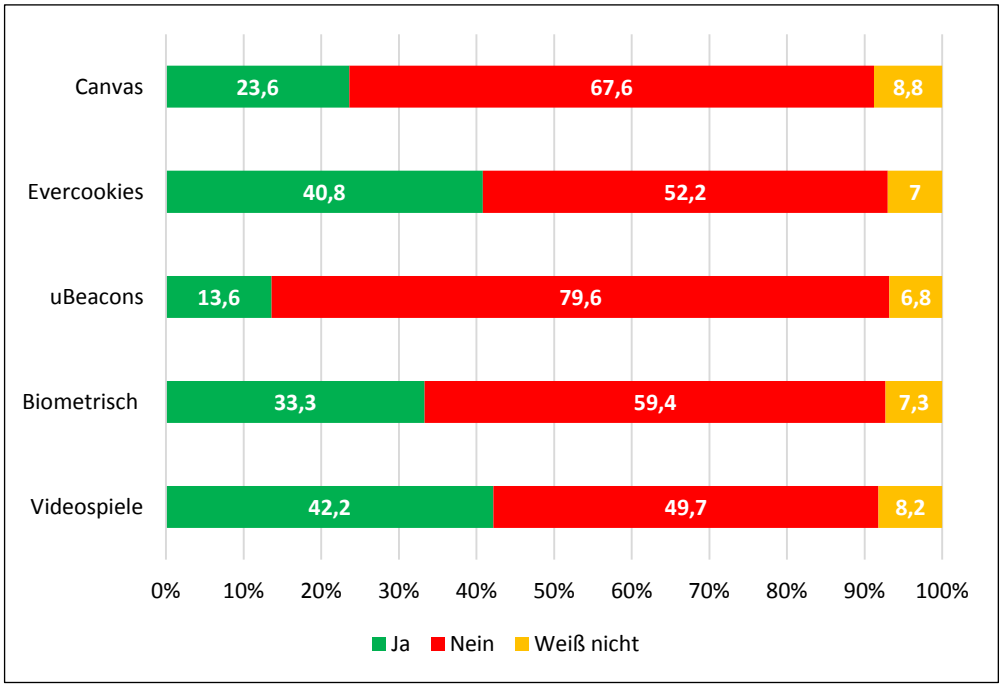


Abb. 01 Kennen Sie folgendes Tracking-Verfahren...?

Um zu überprüfen, welche Einstellung Nutzer/-innen zu den Tracking-Verfahren aufweisen, wurde eine Reihe von zusätzlichen Aussagen präsentiert, die von den Teilnehmenden der Umfrage bewertet wurden (siehe Abbildung 2). Da die Tracking-Methoden durchaus auch Vorteile für Nutzer/-innen bieten können, wie beispielsweise hochgradig personalisierte und damit vielleicht relevantere Werbung oder die Wiedererkennung einer Person auf einem neuen Gerät, wurde gefragt, ob die Teilnehmenden die Verfahren als nützlich, bedrohlich oder besorgniserregend bewerteten. Zusätzlich sollte angegeben werden, ob die Proband(inn)en glaubten, von dem jeweiligen Tracking-Verfahren selbst betroffen zu sein. In Abbildung 2 sind die Bewertungen dieser Aussagen zu sehen, wobei von sechs möglichen Antworten (1 = stimme überhaupt nicht zu und 6 = stimme voll und ganz zu) die beiden mittleren (3 = stimme eher nicht zu und 4 = stimme eher zu) entfernt wurden, um unentschlossene Teilnehmerinnen und Teilnehmer von der Analyse auszuschließen. Durch dieses Vorgehen blieben nur Antworten übrig, die eindeutig eine Ablehnung oder eine Befürwortung der Aussage zum Ausdruck brachten. Zusätzlich wurden nur Personen in die Analysen von uBeacons und biometrischem Tracking integriert, die angegeben hatten, ein mobiles Endgerät (z. B. Smartphone) zu nutzen (n = 417) und es wurden nur Personen in die Analyse von Tracking in Videospielen einbezogen, die angegeben hatten, Videospiele zu spielen (n = 298). Insgesamt ergibt sich ein eher negatives Gesamtbild der Einstellungen der Teilnehmenden gegenüber den Tracking-Verfahren. Es stellte sich heraus, dass deutlich mehr Teilnehmende die Tracking-Verfahren als nicht nützlich bewerteten, verglichen mit denen, die die Verfahren als nützlich ansahen. Die Einschätzung, ob die eigenen Daten durch eines der Tracking-Verfahren gesammelt werden, bot ein weniger einheitliches Bild. Es zeigte sich, dass sehr viele Personen der Meinung waren, von Canvas Fingerprinting und Evercookies betroffen zu sein, allerdings glaubten nicht so viele Personen, dass ihre Daten beim Spielen von Videospielen erfasst werden. Beim Tracking durch Ultraschall (uBeacon) sowie durch die Touchscreen-Wischbewegungen waren die

Lager ungefähr ausgeglichen. Außerdem ergaben die Daten, dass die meisten Teilnehmenden die Aussage, ob die jeweiligen Verfahren unbedenklich seien, stark ablehnten. Am stärksten traf dies auf das Ultraschall-Tracking (uBeacon) zu. Schließlich zeigten die erhobenen Daten, dass die Teilnehmenden drei Tracking-Verfahren als besonders besorgniserregend einstuften, nämlich das Canvas Fingerprinting, Evercookies sowie das Ultraschall-Tracking. Lediglich das Aufzeichnen persönlicher Daten bei Videospielen wurde insgesamt als weniger besorgniserregend bewertet. Ergebnisse einer Zusammenhangsanalyse dieser Aussagen ergaben, dass je höher die Teilnehmenden die Wahrscheinlichkeit einschätzten, von einem Tracking-Verfahren betroffen zu sein, ihnen dieses Verfahren desto mehr Sorge bereitete. Unklar bleibt an dieser Stelle, ob die empfundene Betroffenheit die Sorgen fördert oder umgekehrt (oder ob sich Betroffenheit und Bedenken gegenseitig verstärken). Außerdem zeigte sich, dass eine Einschätzung der Verfahren als nützlich mit einer Bewertung der Verfahren als unbedenklich und weniger besorgniserregend einherging. Auch hier können keine Aussagen über die Richtung der Zusammenhänge gemacht werden.

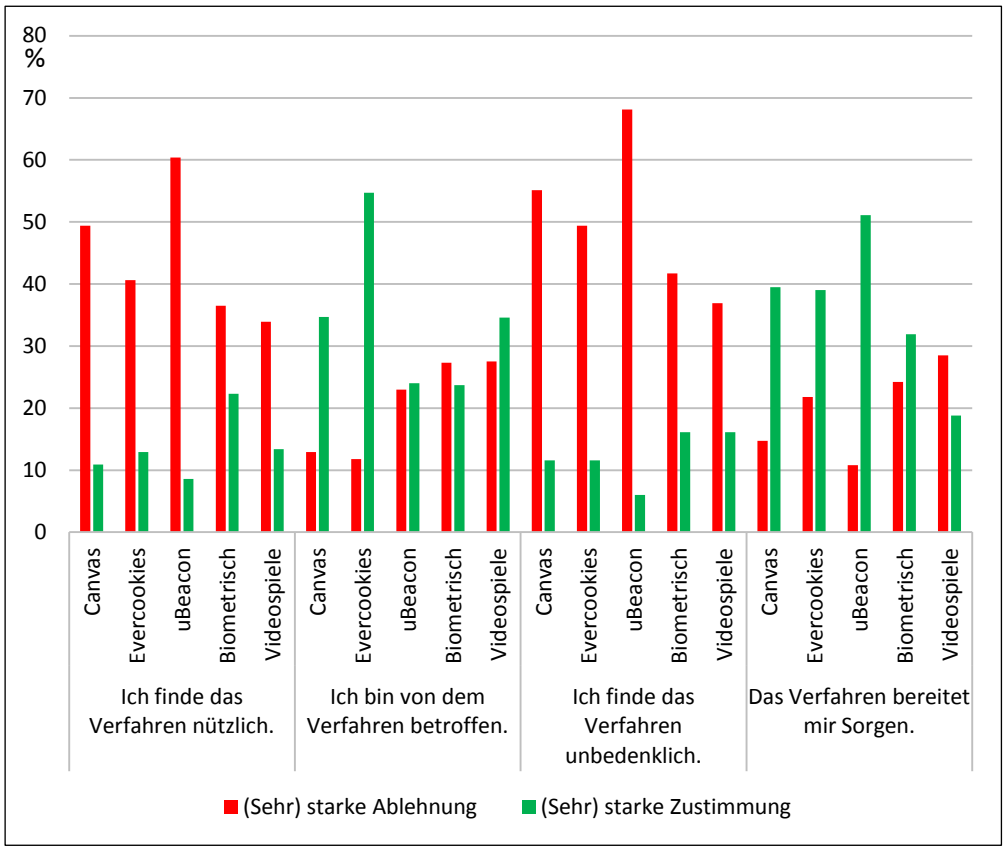
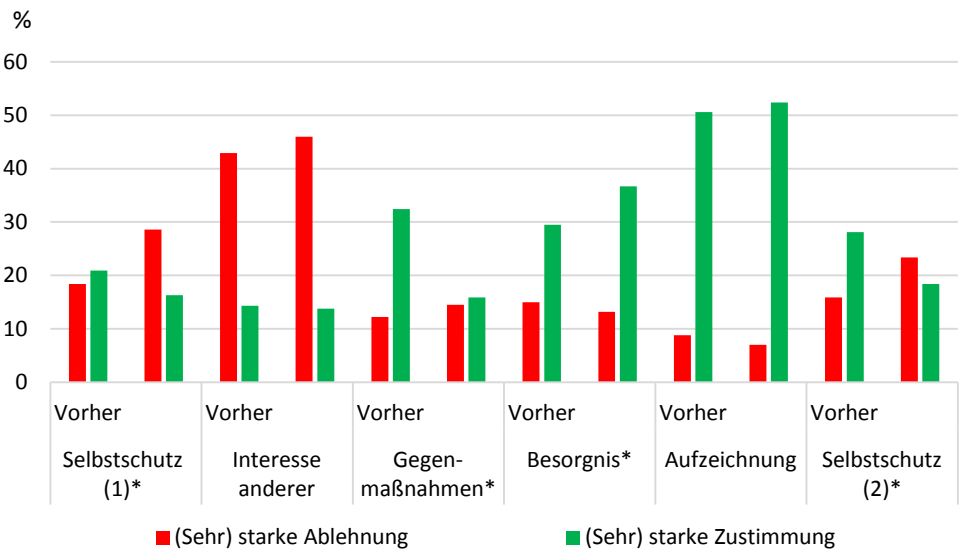


Abb. 02 Bewertung der fünf Tracking-Verfahren

Bevor die Teilnehmenden die Beschreibungen der fünf Tracking-Verfahren durchlasen und ihre Bewertungen diesbezüglich abgaben, bewerteten sie sechs Aussagen. Dieselben Aussagen wurden noch einmal am Ende der Befragung bewertet. Die Aussagen im Wortlaut sowie die Ergebnisse der Bewertung sind in Abbildung 3 dargestellt. Auch hier wurden nur die Antwortkategorien von klarer Ablehnung oder Befürwortung berücksichtigt. Es zeigte sich, dass vier der sechs Aussagen am Ende der Untersuchung anders bewertet wurden als am Anfang. Die Teilnehmenden schätzten ihr Wissen sowie ihre Fähigkeiten, ihre Privatsphäre im Internet zu schützen, am Ende der Untersuchung schlechter ein als am Anfang. Auch war die Bewertung der eigenen Schutzmaßnahmen vor Eingriffen in die Privatsphäre am Ende schlechter als zu Beginn der Studie (bevor die Tracking-Verfahren vorgestellt wurden). Schließlich ergaben die Daten, dass die Teilnehmenden nach der Befragung besorgter um ihre Online-Privatsphäre waren als vor der Befragung. Allerdings glaubten die Befragten vor und nach der Untersu-

chung gleichermaßen, dass ihre Daten im Internet aufgezeichnet werden und dass ihre Daten für andere Parteien interessant sind.



Selbstschutz (1): Ich bin in der Lage meine persönlichen Daten im Internet vor dem Zugriff anderer zu schützen.
Interesse anderer: Ich denke nicht, dass sich jemand für meine persönlichen Daten im Internet interessiert.
Gegenmaßnahmen: Ich ergreife aktive Maßnahmen, um meine persönlichen Daten im Internet zu schützen.
Besorgnis: Grundsätzlich bin ich über meine Privatsphäre besorgt, wenn ich online bin.
Aufzeichnung: Ich glaube, dass alles was ich im Internet tue aufgezeichnet wird.
Selbstschutz (2): Ich besitze das Wissen und die Fähigkeiten meine persönlichen Daten im Internet zu schützen.

* = statistisch signifikanter Mittelwertunterschied ($p < .01$)

Abb. 03 Einschätzung vor und nach der Befragung

Alles in allem lässt sich festhalten, dass die meisten der untersuchten Tracking-Verfahren für den Großteil der Befragten unbekannt waren. Außerdem beurteilte eine Mehrheit der Teilnehmenden die Verfahren als nicht nützlich, als bedenklich und als besorgniserregend. Trotzdem glaubten viele Nutzende, dass sie selbst von den meisten Tracking-Methoden nicht betroffen seien. Schlussendlich ergab die Umfrage, dass selbst kurze gebündelte Informationen über neuartige Tracking-Verfahren die Einschätzung der Nutzenden hinsichtlich ihrer eigenen Fähigkeiten und ihres Wissens ihre Privatsphäre online zu schützen und der allgemeinen Online-Datensammlung leicht beeinflussen können – in die Richtung, dass Personen durch die erhöhte Kenntnis besorgter werden. Hieran lässt sich ansatzweise erkennen, welchen Einfluss Informationen auf die Wahrnehmung von Menschen haben können. Zwar ist noch unklar, ob Wissen alleine überhaupt einen Einfluss auf gezeigtes Verhalten hat, allerdings ist Wissen eine wichtige Grundlage für eine realistische Einschätzung der Menschen, welche privaten Daten wann, wo, von wem und zu welchem Zweck gesammelt werden sowie für den Selbstschutz persönlicher Informationen. Auch im Prozessmodell zur Entwicklung von privatheitsrelevantem Verhalten von Masur und Kollegen[90] bildet das Bewusstsein beziehungsweise Wissen über Privatheitsrisiken die erste Stufe. Sollten Nutzer/-innen der verschiedensten Anwendungen, Dienste und Geräte weiterhin nicht wissen, dass ihr Verhalten nachverfolgt werden kann und wird, kann dieses Unwissen von Unternehmen oder Regierungen leicht missbraucht werden.

Bewertung

Das geringe Wissen über Tracking-Verfahren sowie die überwiegend negative Bewertung derselben durch Nutzer/-innen digitaler Medien deutet auf die Wichtigkeit rechtlicher Regelungen hinsichtlich des Trackings hin. Diese Regelungen sollen im Folgenden genauer beschrieben werden. Dabei liegt ein besonderer Fokus auf der Bewertung der Zulässigkeit des oben bereits angesprochenen Ultraschall-Trackings.

3.4 Rechtliche Regelungen

Die rechtliche Regelung des Tracking wird mit dem Geltungsbeginn der Datenschutz-Grundverordnung (DSGVO)[91] und der geplanten Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation (ePrivacy-Verordnung)[92] eine grundlegende Änderung erfahren. Die Spezialbestimmungen des Telemediengesetzes (TMG)[93] zum Tracking werden durch die allgemeinen Regelungen der Datenschutz-Grundverordnung und die spezifischen Regelungen der ePrivacy-Verordnung ersetzt.

3.4.1 Regelungen im Telemediengesetz

Bisher gilt für Unternehmen in Deutschland, die ihre Nutzende im Internet tracken, um Profiling zu betreiben, das Telemediengesetz, das ein eigenes Regelwerk für die Erstellung von Nutzungsprofilen enthält. § 15 Abs. 3 TMG erlaubt den Dienstanbietern, für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile unter Verwendung von Pseudonymen ohne Einwilligung des Nutzers zu erstellen, sofern der Nutzer nicht widerspricht.[94] Werden allerdings mittels Tracking Nutzungsprofile erstellt, die personenbezogene Daten enthalten, ist deren Erhebung und Verarbeitung nur mit Einwilligung des Betroffenen zulässig.[95] Um zu verhindern, dass Diensteanbieter pseudonymisierte Nutzungsprofile nachträglich der betroffenen Person zuordnen können, gilt das sogenannte Zusammenführungsverbot nach § 15 Abs. 3 Satz 3 TMG, das durch technisch-organisatorische Maßnahmen nach § 13 Abs. 4 Nr. 6 TMG abzusichern ist. Nach § 13 Abs. 1 S. 1 TMG hat der Diensteanbieter die Nutzenden zu Beginn über Art, Umfang, Zweck der Erhebung und Verwendung der personenbezogenen Daten zu unterrichten. Nach Satz 2 erstreckt sich diese Pflicht auch auf automatisierte (programmgesteuerte) Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und den Umgang mit personenbezogenen Daten vorbereiten.[96]

Mit dem Geltungsbeginn der Datenschutz-Grundverordnung müssen die Regelungen des Telemediengesetzes zum Tracking der Verordnung weichen. Die Datenschutz-Grundverordnung sieht weder für Zwecke der Werbung, der Marktforschung noch für die bedarfsgerechte Gestaltung eine pseudonyme Datenverarbeitung vor. Diese Einschränkung der Datenverarbeitung widerspricht zum einen den Erlaubnistatbeständen in Art. 6 Abs. 1 DSGVO und zum anderen dem Zweckbindungsprinzip in Art. 5 Abs. 1 lit. b und Art. 6 Abs. 4 DSGVO. Dies führt dazu, dass § 15 Abs. 3 TMG nicht mehr anwendbar ist und durch die Datenschutz-Grundverordnung verdrängt wird.[97] Da § 15 Abs. 3 TMG nicht mehr anwendbar sein wird, muss dementsprechend auch § 13 Abs. 4 Nr. 6 TMG, der § 15 Abs. 3 Nr. 6 TMG technisch-organisatorisch umsetzt, der Datenschutz-Grundverordnung weichen. Die Datenschutz-Grundverordnung regelt § 13 Abs. 1 TMG entsprechende Informationspflichten in Art. 12 bis 14, jedoch deutlich detaillierter.[98]

3.4.2 Regelungen im Telekommunikationsgesetz

Im Zusammenhang mit dem Betrieb offener WLAN-Netzwerke können über die WLAN-Signale der Smartphones Bewegungsprofile der Nutzer erstellt und verwertet werden (Offline-Tracking). Die Betreiber offener WLAN-Netzwerke stellen zwar keine klassischen Telekommunikations-Diensteanbieter im Sinne des § 3 Nr. 6a TKG dar, da sie dem Kunden keinen eigenen, in der Regel auf eine bestimmte Dauer angelegten Tele-

kommunikationsanschluss überlassen. Das Angebot der Betreiber beschränkt sich nur auf eine kurzzeitige und lokal beschränkte Nutzung des eigenen, vorhandenen Telekommunikationsanschlusses wie z. B. in Kaufhäusern, in Hotels oder Internetcafés, und stellt damit im Regelfall eine Mitwirkung an der Erbringung von Telekommunikationsdiensten im Sinne des § 3 Nr. 6b TKG dar. Somit können die Anbieter offener WLAN-Netze als Diensteanbieter im Sinne des Telekommunikationsgesetzes angesehen werden.[99] Damit erwächst für sie die Pflicht zur Einhaltung des Fernmeldegeheimnisses nach § 88 TKG und des Datenschutzes nach § 91 ff. TKG.

§ 88 Abs. 1 TKG setzt das allgemeine Gebot der Vertraulichkeit der Kommunikation (Vertraulichkeit der Nachrichten und der mit ihnen verbundenen Verkehrsdaten, soweit diese Nachrichten mit öffentlichen Telekommunikations-Netzen und öffentlich zugänglichen Telekommunikations-Diensten übertragen werden) aus Art. 5 Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG - ePrivacy-RL) um.[100] §§ 88 Abs. 2 TKG konkretisiert dieses Vertraulichkeitsgebot, indem er den Diensteanbietern die Pflicht auferlegt, das Fernmeldegeheimnis zu wahren. Dieses umfasst den Inhalt der Telekommunikation und ihre näheren Umstände. Zu diesen zählen alle Verkehrsdaten und sonstigen Umstände, die den jeweiligen Telekommunikationsvorgang individualisierbar machen.[101] Auf die Diensteanbieter wirkt sich das Fernmeldegeheimnis insofern aus, als nach § 88 Abs. 3 Satz 1 TKG der Umgang mit den Daten nur dann erlaubt ist, wenn sie für die Bereitstellung eines Telekommunikationsdienstes einschließlich des Schutzes technischer Systeme erforderlich sind. Nach Satz 3 ist eine Verwertung zu anderen Zwecken nur dann zulässig, wenn dies gesetzlich zulässig ist. Eine Verwertung zu anderen Zwecken wie z. B. zur Leistungs- oder Verhaltenskontrolle und damit zu Zwecken des Tracking ist unzulässig.[102]

Während § 88 TKG eine spezielle Schutzvorschrift für personenbezogene Daten, die im Rahmen eines Telekommunikationsvorgangs anfallen, darstellt, regeln §§ 91 ff. TKG, die auf die ePrivacy-Richtlinie zurückgehen, im welchem Umfang Telekommunikations-Diensteanbieter personenbezogene Daten erheben, verarbeiten und nutzen dürfen.[103]

§ 91 Abs. 1 Satz 1 TKG adressiert Anbieter öffentlicher und nicht-öffentlicher Telekommunikationsdienste, die den Dienst geschäftsmäßig erbringen oder an seiner Erbringung mitwirken. Beim Merkmal der Geschäftsmäßigkeit kommt es nicht auf die Gewerbsmäßigkeit an, sondern darauf, dass der Telekommunikationsdienst dauerhaft ist und nicht auf den Einzelfall begrenzt ist.[104] Ferner ist unerheblich, wie viele Nutzer und wie oft sie den Telekommunikationsdienst nutzen, eine gewisse Regelmäßigkeit aus Sicht des Anbieters muss jedoch vorliegen.[105] Sowohl aufgrund des Kriteriums der Geschäftsmäßigkeit als auch aufgrund der Mitwirkung an der Erbringung des Telekommunikationsdienstes[106] finden §§ 91 ff. TKG nicht nur auf „typische" Telekommunikationsunternehmen, sondern auch auf WLAN-Anbieter Anwendung.

Für den Bereich des (Offline-)Tracking ist § 96 TKG, der die Verarbeitung von Verkehrsdaten nach § 3 Nr. 30 TKG regelt, und § 98 TKG, der dem Umgang mit Standortdaten nach § 3 Nr. 19 TKG reguliert, von Bedeutung. Nach § 96 Abs. 3 TKG ist eine Verarbeitung von Verkehrsdaten zu Zwecken der Vermarktung von Telekommunikationsdiensten, zur bedarfsgerechten Gestaltung von Telekommunikationsdiensten oder zur Bereitstellung von Diensten und damit auch zu Tracking-Zwecken nur mit Einwilligung des Betroffenen oder des Nutzers zulässig und nur im dazu erforderlichen Maß und Umfang. Eine ähnliche Regelung sieht auch § 98 Abs. 1 TKG vor, nach der Standortdaten bei Diensten mit Zusatznutzen nur mit Einwilligung, nur im erforderlichen Umfang und nur innerhalb des erforderlichen Zeitraumes verarbeitet werden dürfen.

3.4.3 Regelungen der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung enthält keine spezifischen Regelungen zum Tracking und der damit einhergehenden Möglichkeit, Profiling zu betreiben. In der Daten-

Bewertung

schutz-Grundverordnung findet sich jedoch eine Reihe allgemeiner Regelungen, die auf Tracking und Profiling anwendbar sein werden.

An dieser Stelle sei darauf hingewiesen, dass alle nationalen datenschutzrechtlichen Vorschriften, die auf die ePrivacy-Richtlinie zurückgehen, trotz des Anwendungsvorrangs der Datenschutz-Grundverordnung ausweislich des Art. 95 DSGVO nicht verdrängt werden und fortgelten.[107] Für das Tracking betrifft dies die Regelung der §§ 88, 91, 96 und 98 TKG.[108] Diese gelten solange fort, bis die ePrivacy-Verordnung in Deutschland wirksam wird und damit die ePrivacy-Richtlinie ersetzt. Die Datenschutz-Grundverordnung gilt also nur, soweit das Tracking nicht durch das Telekommunikationsgesetz erfasst wird.

Terminologisch lässt sich der Begriff „Tracking" unter den mehrfach in der Datenschutz-Grundverordnung verwendeten Begriff „Profiling" fassen.[109] Gemäß der Definition in Art. 4 Nr. 4 DSGVO ist unter Profiling jede Art der automatisierten Verarbeitung personenbezogener Daten zu verstehen, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte, wie etwa die wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen und Verhalten zu analysieren oder vorherzusagen.

Profiling ist – wie jede andere Art der Datenverarbeitung auch – nach Art. 6 Abs. 1 UAbs. 1 DSGVO zulässig, sofern zum Beispiel die betroffene Person in die Verarbeitung nach lit. a eingewilligt hat oder die Verarbeitung nach lit. f zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Das Profiling ist rechtlich zulässig, solange die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, gegenüber den berechtigten Interessen des Verantwortlichen oder eines Dritten nicht überwiegen. Die kollidierenden Interessen des Verantwortlichen und der vom Profiling betroffenen Person sind im Wege einer Interessenabwägung in einen Ausgleich zu bringen.[110]

Der Verantwortliche hat die Pflicht, die betroffene Person bei der Erhebung personenbezogener Daten nach den Vorgaben des Art. 13 oder 14 DSGVO zu informieren, abhängig davon, ob personenbezogene Daten bei der betroffenen Person erhoben wurden oder bei Dritten. Zudem muss der Verantwortliche sicherstellen, dass die betroffene Person ihr Auskunftsrecht nach Art. 15 DSGVO, das Recht auf Berichtigung nach Art. 16 DSGVO, das Recht auf Löschung nach Art. 17 DSGVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO sowie das Recht auf Datenübertragbarkeit nach Art. 20 DSGVO wahrnehmen kann. Zudem hat die betroffene Person ein Widerspruchsrecht nach Art. 21 DSGVO. So kann die betroffene Person nach Art. 21 Abs. 1 Satz 1 DSGVO einer auf Profiling gestützten Datenverarbeitung widersprechen, wenn die Datenverarbeitung auf Grund von Art. 6 Abs. 1 UAbs. 1 lit. e und f DSGVO erfolgt. Zudem besteht ein Widerspruchsrecht nach Art. 21 Abs. 2 S. 2 DSGVO, wenn das Profiling mit Direktwerbung in Verbindung steht. Während Art. 21 DSGVO in Abs. 2 für Direktwerbung ein voraussetzungsloses Widerspruchsrecht normiert, bedarf es im Rahmen des Abs. 1 zusätzlicher Gründe, die sich aus der besonderen Situation der betroffenen Person ergeben, die einen Widerspruch rechtfertigen können. Im Gegensatz zum bisher geltenden Telemediengesetz entfällt künftig somit ein voraussetzungsloses Widerspruchsrecht, wenn die Datenverarbeitung zu Zwecken der bedarfsgerechten Gestaltung oder der Marktforschung erfolgt.[111]

Hat der Verantwortliche die personenbezogenen Daten rechtmäßig erhoben und zu einem Profil zusammengeführt oder dieses Profil rechtmäßig erhalten, stellt sich die Frage, ob und für welche Zwecke er das Profil verwenden darf. Hier kann das Verbot des Art. 22 Abs. 1 DSGVO greifen. Diese Vorschrift regelt die automatisierte Entscheidung im Einzelfall einschließlich Profiling. Nach ihr hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Erwägungsgrund 71 nennt hier als Beispiele die automatische Ablehnung eines Online-

Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen. Dieses Recht der betroffenen Person besteht hingegen nach Art. 22 Abs. 2 DSGVO nicht, wenn dies für den Abschluss oder die Erfüllung eines Vertrags erforderlich ist, sich aus anderen Rechtsvorschriften, die die Rechte der betroffenen Person ausreichend wahrt, aus einer spezifischen Rechtsgrundlage ergibt oder die betroffene Person in die Verarbeitung eingewilligt hat. Art. 22 DSGVO findet auf das Tracking zu Werbezwecken oder zur Personalisierung von Diensten keine Anwendung, da dies der betroffenen Person gegenüber keine rechtlichen Wirkungen entfaltet oder in ähnlicher Weise erheblich beeinträchtigt.[112]

Die Datenschutz-Grundverordnung findet auch auf pseudonymisierte Nutzungsprofile Anwendung.[113] Im Gegensatz zu den Regelungen des Telemediengesetzes besteht nach Wirksamwerden der Datenschutz-Grundverordnung jedoch keine explizite Pflicht mehr, die Daten zu pseudonymisieren. Allerdings kann die Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 dazu führen, dass die schutzwürdigen Interessen der betroffenen Person nur dann gegenüber den berechtigten Interessen des Verantwortlichen nicht überwiegen, wenn die Daten der betroffenen Person pseudonym verarbeitet werden. Art. 4 Nr. 5 DSGVO enthält eine Legaldefinition für den Begriff der Pseudonymisierung. Darunter wird die Verarbeitung von personenbezogenen Daten in einer Weise verstanden, dass die personenbezogenen Daten ohne die Heranziehung weiterer Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.[114] Aus der Begriffsbestimmung lässt sich ferner entnehmen, dass die zusätzlichen Informationen gesondert aufzubewahren sowie technische und organisatorische Maßnahmen zu ergreifen sind, die sicherstellen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden können. Hieraus ergibt sich implizit auch ein Zusammenführungsverbot der Nutzungsprofile mit den weiteren separat aufbewahrten Informationen, um eine nachträgliche Identifizierung der betroffenen Person zu verhindern.[115] Die Informationspflichten des Verantwortlichen sowie die Rechte der betroffenen Person gelten auch für pseudonymisierte Nutzungsprofile, die für den Verantwortlichen personenbeziehbar sind.

3.4.4 Regelungen im Entwurf einer ePrivacy-Verordnung

Die ePrivacy-Verordnung soll die Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG) ablösen und sollte ursprünglich zeitgleich mit der Datenschutz-Grundverordnung am 25. Mai 2018 Geltung erlangen. Inzwischen zeichnet sich jedoch ab, dass der ambitionierte Zeitplan für das Inkrafttreten der ePrivacy-Verordnung wohl nicht zu halten ist.[116] Bisher liegen der Entwurf der Kommission vom 10.1.2017[117] und die Stellungnahme des Parlaments vom 23.10.2017[118] vor. Die Entschließung des Rats wird für den Sommer 2018 erwartet. Danach schließt sich noch der Trilog an, in dem zwischen Rat und Parlament unter Beteiligung der Kommission nach einem Kompromiss zwischen den drei Entwürfen gesucht wird. Mit einer Verabschiedung der ePrivacy-Verordnung ist daher vor Ende 2018 kaum zu rechnen.[119]

Die ePrivacy-Verordnung ist eine Spezialregelung zur Datenschutz-Grundverordnung, die sie im Bereich der elektronischen Kommunikation präzisieren und ergänzen soll.[120] Sie geht in ihrem Anwendungsbereich der Datenschutz-Grundverordnung vor.

Art. 6 ePrivacy-VO-E des aktuellen Entwurfs zur Verordnung regelt die Verarbeitung elektronischer Kommunikationsdaten. Die Regelung umfasst sowohl elektronische Kommunikationsinhalte[121] als auch elektronische Kommunikationsmetadaten.[122] Während Art. 7 ePrivacy-VO-E die Speicherung und Löschung elektronischer Kommunikationsdaten regelt, normiert Art. 8 ePrivacy-VO-E in Abs. 1 das Tracking im Internet und in Abs. 2 das Offline-Tracking.

Für die Nutzung von Informationen aus Endeinrichtungen,[123] anhand derer das Tracking der Nutzer im Internet ermöglicht wird, schreibt Art. 8 Abs. 1 lit. b ePrivacy-VO-E die Einwilligung der Nutzer vor. Anders als bei der Datenschutz-Grundverordnung ge-

nügt es hier nicht, dass die Interessen der betroffenen Person gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen. Das Einwilligungserfordernis gilt für jede vom jeweiligen Nutzer nicht selbst vorgenommene Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer (vor allem Computer, Smartphones und Tablets),[124] auch über deren Software und Hardware. Für die Einwilligung sind die Vorschriften der Datenschutz-Grundverordnung (Art. 4 Nr. 11 und Art. 7) zu beachten.

Ausnahmen vom Einwilligungserfordernis sind nach Art. 8 Abs. 1 ePrivacy-VO-E in engen Grenzen wie zur Durchführung eines elektronischen Kommunikationsvorgangs (lit. a) oder zur Bereitstellung eines vom Endnutzer gewünschten Dienstes der Informationsgesellschaft (lit. c) möglich. Zu den vom Endnutzer gewünschten Diensten der Informationsgesellschaft gehört vor allem die Warenkorbfunktion eines Online-Shops.[125] Ferner statuiert der ePrivacy-VO-E in lit. d eine Ausnahme für die Messung des Webpublikums. Die Ausnahme gilt dann, wenn der Webseitenbetreiber des vom Endnutzer gewünschten Dienstes diese Messung selbst durchführt, in seinem Namen oder von einem unabhängigen, vom Betreiber beauftragten Webanalysedienst, der im öffentlichen Interesse oder für wissenschaftliche Zwecke tätig ist, durchführen lässt. Voraussetzung hierfür ist, dass dem Nutzer die Möglichkeit eingeräumt wird, der Nutzung zu widersprechen und dass personenbezogene Daten keinem Dritten zugänglich gemacht werden. Auch dürfen die Grundrechte der Nutzenden durch eine Messung nach lit. d nicht beeinträchtigt werden.

Ferner sieht Art. 8 ePrivacy-VO-E in Abs. 1a ein Verbot von sogenannten Tracking-Walls vor. Webseitenbetreiber dürfen den Nutzern den Zutritt zu ihren Webseiten nicht verweigern, wenn sie ins Tracking nicht einwilligen oder die Einwilligung nachträglich widerrufen.

Im Hinblick auf Art. 8 Abs. 1 ePrivacy-VO-E lässt sich einerseits folgern, dass jede Form des Webtrackings – unabhängig ob Cookies, Fingerprints oder ähnliche Technologien – von dem Entwurf der ePrivacy-VO-E umfasst ist, und zwar unabhängig davon, ob personenbezogene oder nicht-personenbezogene Daten verarbeitet werden. Art. 8 regelt allerdings nicht die weitere Verarbeitung zulässig erhobener Trackingdaten. Ob diese z.B. zu Nutzungsprofilen zusammengefasst werden dürfen, ist nach den Regeln der Datenschutz-Grundverordnung zu entscheiden.[126]

Während Art. 8 Abs. 1 ePrivacy-VO-E Fälle von Online-Tracking über den gesteuerten Zugriff auf Endgeräteinformationen umfasst, regulieren Art. 8 Abs. 2 und 2a DSGVO den Datenaustausch zwischen Maschine und Maschine, der unter anderem für das Offline-Tracking von Funkverbindungen mobiler Endgeräte von Relevanz ist.[127] Das Tracking für die Erstellung von Bewegungsprofilen von Nutzer/innen zum Beispiel beim Shopping in Innenstädten oder auf Flughäfen (sog. Retail-Tracking) über WLAN- und Bluetooth-Signale mobiler Endgeräte ist nach Abs. 2 UAbs. 1 nur mit Einwilligung des Nutzers (lit. aa) möglich oder wenn die Risiken eingedämmt werden (lit. ab). Für letzteres müssen nach Abs. 2a die Daten ausschließlich für statistische Zählungen (lit. a) verwendet werden, räumlich und zeitlich begrenzt sein (lit. b) und unverzüglich nach Erfüllung des Zwecks gelöscht oder anonymisiert werden (lit. c). Außerdem muss dem Nutzer eine effektive Widerrufsmöglichkeit eingeräumt werden (lit. d). Im Ergebnis bedeutet das, dass sofern die Nutzenden in das Offline-Tracking nicht ausdrücklich einwilligen, die Erstellung von individuellen Bewegungsprofilen rechtlich nicht zulässig ist.

Mit der in Art. 8 ePrivacy-VO-E geplanten Regelung zum Tracking erfasst die ePrivacy-Verordnung einen sensiblen Bereich und stößt dabei auf Kritik von verschiedenen Seiten.[128] Von den Interessenvertretern der Digitalwirtschaft wird kritisiert, dass die ePrivacy-Verordnung die Nutzung in Endgeräten im Bereich der Verarbeitungs- und Speicherfunktion auf das Nötigste reduziert und damit die Möglichkeit erheblich einschränkt, Online-Angebote zu personalisieren oder leichter bedienbar zu machen.[129] Die Verlagsbranche befürchtet einen erheblichen Umsatzrückgang und fordert eine

Lockerung der strickten Regulierung zu Tracking. Diese verhindert, den Nutzern personalisierte Werbung anzuzeigen und entzieht damit den Verlagen die Grundlage für ihr Geschäftsmodell.[130]

Im Gegensatz zu den Stimmen der Digitalindustrie und Verlage fordert der Europäische Datenschutzbeauftrage einen eindeutigen Ausschluss von Tracking.[131] Ferner spricht sich Art. 29-Datenschutz-Gruppe zum einen dafür aus, für jede Webseite oder Applikation „Tracking-Ziele" einzeln konkret festzulegen und die geplante unspezifische Zustimmung zu allen Tracking-Verfahren zu streichen. Zum anderen fordert sie, das geplante Verbot von „Tracking-Walls" durchzusetzen.[132]

Auch wenn die Arbeiten an der ePrivacy-Verordnung zügig voranschreiten und der Entwurf ein Tauziehen zwischen verschieden Interessensvertretern hervorruft, zeichnet sich mittlerweile ab, dass die ePrivacy-Verordnung frühestens im Jahr 2019 zur Geltung kommen wird. Die Zulässigkeit von Tracking wird sich in der Zeit vom 25. Mai 2018 (Geltungsbeginn der DSGVO) bis zum Geltungsbeginn der ePrivacy-Verordnung – abgesehen von der Einwilligung – nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO orientieren, wonach eine Abwägung der betroffenen Interessen des Verantwortlichen oder eines Dritten mit den Interessen der betroffenen Person durchzuführen ist. Eine Übergangsfrist, so wie es bei der Datenschutz-Grundverordnung der Fall ist, ist für die ePrivacy-Verordnung nicht vorgesehen.

3.4.5 Zulässigkeit von Tracking am Beispiel von Ultraschall-Tracking

Gerade bei den neuen Trackingmethoden, die als besonders eingriffsintensiv bezeichnet werden können, stellt sich die Frage, ob ihre Nutzung zu Zwecken des Trackings zulässig ist. Im Fall des Ultraschall-Trackings, dessen technische Funktionsweise in Kapitel 2.6.2 beschrieben wurde, geht es um die Verknüpfung der Erkenntnisse zu verschiedenen Endgeräten und umfangreiche Analysen des Nutzungsverhaltens mit diesen Geräten und den genutzten Plattformen. Dadurch ist es dem Anbieter etwa zur Bestimmung von für die Nutzenden möglicherweise relevanten Inhalten und Werbung nicht nur möglich, auf die Nutzung an einem Endgerät abzustellen, sondern er kann die Nutzung über viele verschiedene Endgeräte in einem zentralen Nutzerprofil zusammenführen.

Bei der Frage nach einschlägigen Rechtsgrundlagen für diese Datenverarbeitung durch Tracking ist zunächst die Anwendbarkeit der Datenschutz-Grundverordnung zu klären. Wie bereits erläutert, wird sich die Rechtmäßigkeit von Offline-Tracking in Zukunft in der Regel an den Vorschriften der ePrivacy-Verordnung messen lassen müssen. Solange die ePrivacy-Verordnung allerdings noch nicht beschlossen wurde, sind die allgemeinen Regelungen der Datenschutz-Grundverordnung sowie die bestehende ePrivacy-Richtlinie und die sie umsetzenden nationalen Gesetze anwendbar. Mit Anwendbarkeit der ePrivacy-Verordnung wird sich der Verantwortliche – nach aktuellem Stand der Entwurfsfassung - nur noch auf die Einwilligung als Rechtsgrundlage berufen können. Art. 95 DSGVO und der Vorrang der ePrivacy-Richtlinie gilt nicht, weil Offline-Tracking von dieser Richtlinie nicht erfasst wird. Für die Datenverarbeitung während des Ultraschall-Trackings kommen nach Datenschutz-Grundverordnung prinzipiell zwei Rechtsgrundlagen in Frage, einerseits die Einwilligung aus Art. 6 Abs. 1 UAbs. lit. a DSGVO und die Möglichkeit des Verantwortlichen nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO, sich auf die Ausübung berechtigter Interessen zu berufen.

Gerade bei der Einwilligung offenbaren sich aber bereits auf den ersten Blick umfassende Probleme. So setzt eine Einwilligung nach Art. 4 Nr. 11 DSGVO eine freiwillige, bestimmte, informierte und unmissverständliche Willensbekundung der betroffenen Person voraus, mit der sie ihr Einverständnis in die Verarbeitung der sie betreffenden personenbezogenen Daten zum Ausdruck bringt. Dies setzt voraus, dass das Einverständnis im konkreten Einzelfall des Aussendens der identifizierenden Merkmale sowie des Empfangens und der Suche nach diesen Merkmalen eingeholt wird. Hierzu muss der Nutzer über den Zeitpunkt der Identifikation, das Ausmaß und den Inhalt der aus-

Bewertung

getauschten Informationen und die jeweiligen Zwecke der Datenverarbeitung hinreichend informiert sein. Durch diese Anforderungen wäre es für den Verantwortlichen nicht mehr möglich, ein Tracking „hinter dem Rücken" des Nutzers durchzuführen. Gerade die Anforderung, dass für die Datenerhebung und -verarbeitung auf sämtlichen zusammenzuführenden Geräten eine entsprechende Einwilligung existieren muss, würde dazu führen, dass die Nutzenden de facto eine händische Koppelung der Geräte vorzunehmen haben. Wenn das Profiling auch der Nutzungsauswertung zur Finanzierung kostenfreier Dienste dient, dürfte es für die Annahme einer Einwilligung durch den Verstoß gegen das Koppelungsverbot in Art. 7 Abs. 4 DSGVO auch an der notwendigen Freiwilligkeit scheitern.

Soweit sich der Verantwortliche auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO beruft, so müsste er zunächst ein berechtigtes Interesse geltend machen. Auf Grundlage des weiten Wortlautes der Norm ist darunter jedes rechtlich in irgendeiner Weise geschützte Interesse zu verstehen. Daher handelt es sich auch bei dem Interesse des Verantwortlichen, die Nutzenden eines Dienstes zu werblichen Zwecken zu tracken und die Nutzungsprofile über verschiedene Mobilgeräte hinweg zusammenzuführen, um eine solche erweiterte Analyse des Nutzerverhaltens durchführen zu können, um ein berechtigtes gewerbliches Interesse im Sinne dieser Vorschrift. Der Verantwortliche kann sich für diese Tätigkeit auf seine Berufsfreiheit nach Art. 12 Abs. 1 GG und Art. 15 Abs. 1 und 2 GRCh berufen.

Das Ultraschall-Tracking müsste zur Wahrnehmung des berechtigten Interesses erforderlich sein. Es darf nicht mit weniger intensiver Datenverarbeitung in etwa gleichem Maße erreicht werden können. Im Regelfall kann der Anbieter auch ohne Ultraschall-Tracking das Nutzerverhalten über verschiedene Geräte gleich zuverlässig zusammenführen. Dies ist jedenfalls immer dann der Fall, wenn sie der Nutzer auf jedem Gerät separat mit dem jeweiligen Dienst anmeldet. Allerdings ist es dem Anbieter nicht möglich, ihm bislang fremde Geräte in einer von der Entscheidung des Nutzers im Einzelfall abgekoppelten Weise zu „erkennen". Hier könnte von Anbieterseite vertreten werden, dass gerade dieses Erkennen der Nutzergeräte ohne entsprechendes Login der Nutzenden für das berechtigte Geschäftsinteresse des Anbieters erforderlich ist.

Problematisch ist allerdings darüber hinaus, dass der Anbieter, während das jeweilige Endgerät nach Identifikatoren anderer Endgeräte im Ultraschall-Frequenzbereich „horcht", über die konkret zur Erkennung der anderen Endgeräte notwendigen Daten hinaus auch noch weitere, zur Erreichung des Zweckes nicht notwendige, Daten erhebt und verarbeitet, nämlich die Umgebungsgeräusche im hörbaren Frequenzbereich und womöglich Identifikatoren anderer Geräte fremder Nutzer, die im Umfeld ebenfalls im Ultraschall-Frequenzbereich ausgesendet werden.

Nicht erforderlich für das genannte berechtigte Interesse des Verantwortlichen ist es, das Ultraschall-Tracking heimlich und ohne besondere Information der betroffenen Person durchzuführen. Heimliches Offline-Tracking ist somit nicht zulässig.
Im Rahmen der Interessenabwägung kann sich die betroffene Person auf Art. 7 und 8 GRCh berufen. In der Regel wird man für das Ultraschall-Tracking zu dem Ergebnis kommen, dass die Interessen, Rechte und Grundfreiheiten der betroffenen Personen gegenüber dem berechtigten Interesse des Verantwortlichen überwiegen. So muss einerseits beachtet werden, dass sowohl die Gefahr des „Beifangs" von nicht relevanten Informationen besteht und dies sowohl von der betroffenen Person als auch von betroffenen Dritten. Andererseits besteht auch in Fällen des geräteübergreifenden Trackings bei der Nutzung von Diensten, zu denen sich der Nutzer anmelden muss, die Möglichkeit des Diensteanbieters, eine Anbindung der unterschiedlichen Endgeräte durch die Nutzenden herbeizuführen. Denn zu Gunsten der Nutzenden muss diesen auch die Möglichkeit eines selbstbestimmten Identitätsmanagements eingeräumt werden. Sofern eine solche Verknüpfung durch die Nutzenden nicht manuell geschieht, ist jedenfalls kein gleichwertiges oder höherrangiges Interesse des Verantwortlichen ersichtlich, das die bewusste Entscheidung der Nutzenden überstimmen können sollte.

Bewertung

Insbesondere ist nicht ersichtlich, dass Nutzende bei der Nutzung kostenloser Dienste davon auszugehen haben, dass der Diensteanbieter durch kontinuierliche Audioüberwachung praktisch ein Fenster in eine intime Sphäre ihres Lebens erhält. Hierbei ist besonders zu beachten, dass den Nutzenden die detaillierte technische Funktionsweise und das Ausmaß der Nutzung in der Regel nicht bekannt ist. Dies birgt auch die Gefahr der Deanonymisierung und des Missbrauchs dieser Technologien durch Dritte.
Nach alledem kann sich der Verantwortliche für Ultraschall-Tracking zu Zwecken der Werbung in der Regel nicht auf die Ausübung berechtigter Interessen berufen. Die Zulässigkeit eines auf Einwilligung basierenden geräteübergreifenden Trackings hängt von der konkreten Umsetzung des Trackings und der Einholung der Einwilligung ab. Die Möglichkeiten eines zulässigen Trackings sind jedoch durch die rechtlichen Anforderungen deutlich eingeschränkt und daher in der Praxis vermutlich unattraktiv.

4
Empfehlungen

4.1 Technische Empfehlungen

Der folgende Abschnitt widmet sich Empfehlungen zum Umgang mit Tracking-Verfahren. Diese Empfehlungen werden aus technischer sowie rechtswissenschaftlicher Perspektive angesprochen. Erstere setzt in erster Linie bei softwarebasierten Maßnahmen an, welche dem Schutz und der Abwehr von Tracking dienen. Hierbei muss wiederum zwischen zwei Ansätzen unterschieden werden, nämlich das browserbasierte Blocken sowie das Blocken auf Netzwerkebene.

Für die meisten Browser gibt es Erweiterungen, die unerwünschte Werbung und heimliches Tracking blockieren. Da diese direkt im Browser realisiert werden, haben sie Zugriff auf Ressourcen der jeweils aufgerufenen Webseite. Sie können Skripte und Anfragen an externe Server untersuchen und blockieren oder Antworten manipulieren. Ein erprobter Ansatz ist die Nutzung von Filterlisten mit bekannten Trackern. Diese können von der Nutzergemeinschaft via Crowdsourcing, vom Entwickler des Plugins oder automatisiert oder algorithmisch erstellt werden.[133] Bekannte Tracking-Blocker, welche auf manuell erstellen Filterlisten basieren, sind AdBlock Plus, uBlock, Ghostery, Blur oder Disconnect.

Beim netzwerkbasiertem Blocken wird versucht, das Laden von Werbung und Trackingskripten durch die Modifikation und Blockierung von Paketen zu verhindern. Da dies nicht im Browser, sondern auf Netzwerkebene geschieht, ist netzwerkbasiertes Blocken unabhängig vom genutzten Browser und kann Werbung aus Anwendungen und Apps filtern. Allerdings ist es nicht immer möglich, auf Netzwerkebene noch zu entscheiden, ob eine Anfrage an eine Drittpartei vom Nutzer erwünscht ist oder nicht.
Ein bei Smartphones beliebter Ansatz ist das DNS-Blocking. Über das Domain Name System (DNS) kann ein Rechner eine Domain in eine IP-Adresse auflösen. Beim DNS-Blocking werden alle Anfragen an das DNS, deren Adresse sich auf einer schwarzen Liste befindet, bewusst falsch beantwortet. Auf diese Weise lassen sich jedoch nur ganze Domains beziehungsweise ganze Subdomains blockieren. Ein unerwünschtes Skript, das über die gleiche Domain wie der erwünschte Inhalt zu erreichen ist, lässt sich mit DNS-Blocking nicht blockieren, ohne dass der Inhalt ebenfalls blockiert würde.[134] Ein Beispiel hierfür ist die Android App „AdAway".[135] DNS-Blocking lässt sich aber auch netzwerkweit anwenden. Die Software „Pi-Hole" lässt sich beispielsweise auf einen Server oder auf den namensgebenden Einplatinencomputer Raspberry Pi aufspielen. Im Anschluss konfiguriert man seinen Router so, dass er DNS-Anfragen zu Pi-Hole weiterleitet. Pi-Hole entscheidet dann anhand einer Filterliste, ob die Anfrage richtig beantwortet wird. Das hat den Vorteil, dass man über den Server ähnlich einer Firewall zentral blocken kann. Firmen, Universitäten oder private Nutzer/-innen mit mehreren Geräten können somit unabhängig von den Endgeräten bestimmte (Sub-)Domains blockieren. Dies beinhaltet auch Geräte wie Smart-TVs, auf denen man keinen Blocker installieren kann.[136]

Ferner bestehen existierende Lösungen zum Schutz vor Tracking für mobile Endgeräte in der Regel aus alternativen Browser-Apps wie „Cliqz", der App „Adblock Browser" oder Erweiterungen beziehungsweise Modifizierungen des mobilen Betriebssystems. [137] [138] Ad- und Tracking-Blocker als Browser-Apps sind typischerweise Umsetzungen bestehender Lösungen für PC und Laptop und greifen beim mobilen Tracking nur bedingt. Tatsächlich ist die Effektivität derartiger Browser-Apps fragwürdig, da sie ausschließlich auf das mobile Browsing fokussiert sind. Sie berücksichtigen kaum die Tatsache, dass andere Onlinedienste überwiegend über Apps genutzt werden.

4.2 Rechtliche Empfehlungen

Neben der Möglichkeit, sich über technische Verfahren vor möglichen Tracking-Anwendungen zu schützen, bestehen zudem Möglichkeiten, rechtlich das Tracking einzuschränken oder eventuell zu verbieten. Bereits im Entwurf einer ePrivacy-Verordnung des Parlaments ist der Do-Not-Tracking-Grundsatz aufgenommen. Tracking soll grundsätzlich verboten und nur innerhalb enger gesetzlicher Grenzen erlaubt sein – vor allem dann, wenn der Nutzer darin eingewilligt hat. Dadurch kommt der Einwilligung in der Praxis eine hohe Bedeutung zu. Die wohl relevanteste gesetzliche Erlaubnis für Tracking dürfte sich auf technische Notwendigkeiten, wie zum Beispiel das Setzen von Cookies für die Warenkorbfunktion oder für Konfigurationszwecke, beziehen.

Die beiden Entwürfe beschränken sich auf die Endgeräte der Nutzer. Sie regeln nur die Daten, die auf dem Endgerät erhoben, verarbeitet und zum Tracking-Verantwortlichen übertragen werden. Der Großteil der Datenverarbeitung, der auf den Servern des Tracking-Verantwortlichen erfolgt, bleibt hingegen von dem Entwurf der ePrivacy-Verordnung unberücksichtigt. Hierfür werden die allgemeinen Vorschriften der Datenschutz-Grundverordnung Anwendung finden. Wünschenswert wäre in diesem Zusammenhang eine Ausweitung der ePrivacy-Verordnung auch auf die Datenverarbeitung auf den Servern des Tracking-Verantwortlichen. Bis dahin wird sich die Zulässigkeit der sich an das Tracking anschließenden Datenverarbeitung auf den Servern des Verantwortlichen vorrangig nach der Interessenabwägung des Art. 6 Abs. 1 lit. f DSGVO richten. Bis konkrete Vorgaben durch den Europäischen Datenschutzausschuss oder Gerichtsentscheidungen vorliegen, sind die Verantwortlichen auf der sicheren Seite, wenn sie vorrangig die Einwilligung der betroffenen Person einholen und ausschließlich pseudonyme Profile nutzen.

Zudem unterscheidet der Entwurf der ePrivacy-VO nicht zwischen pseudonymen und personenbezogenen Nutzerprofilen. Hier sollten Anreize für Tracking-Verantwortliche vorgesehen werden, vorrangig pseudonymisierte Nutzerprofile zu verwenden, da diese mit geringeren Risiken für die Grundrechte der betroffenen Person verbunden sind. Wünschenswert wäre es, wenn das Europäische Parlament mit seinem Vorschlag Erfolg hat, weitere Erlaubnisnormen hinsichtlich der Messung des Webpublikums nach Art. 8 Abs. 1 lit. d ePrivacy-VO-E aufzunehmen. Nach dieser Vorschrift sollen derartige Messungen nach Art. 8 Abs. 1 lit. da, i bis iii ePrivacy-VO-E, zulässig sein, um Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Endeinrichtungen des Endnutzers zu wahren. Dabei dürfen jedoch die Funktionsweise der Hardware oder Software oder die von den Nutzenden festgelegten Einstellungen zum Schutz der Privatsphäre nicht geändert werden. Auch müssen die Nutzenden bei jeder Installation eines Updates im Voraus informiert werden sowie die Möglichkeit haben, die automatische Installation des Updates zu verschieben oder auszuschalten.

Erstrebenswert wäre auch im Hinblick auf die Erteilung der Einwilligung eine deutliche Differenzierung zwischen „immer getrackt werden" und „nie getrackt werden". Einen ähnlichen Vorschlag hat die Kommission gemacht. So schlägt sie ein abgestuftes Einwilligungssystem vor, das einen höheren Schutz (zum Beispiel „Cookies niemals annehmen"), einen mittleren Schutz (zum Beispiel „Cookies von Drittanbietern zurückweisen") und einen niedrigen Schutz („Cookies immer annehmen") kennt.[139] Einen Mehrwert für die Grundrechte der betroffenen Personen würde auch der Vorschlag des Europäischen Parlaments bringen, Tracking Walls zu verbieten, die lediglich die Möglichkeit des „take it or leave it" bieten.

Die Trilog-Verhandlungen zwischen der Kommission, dem Parlament und dem Rat stehen noch aus. Dementsprechend ist nicht abzusehen, wie der finale Wortlaut der ePrivacy-Verordnung aussehen wird. Am grundlegenden Rahmen wird sich jedoch wahrscheinlich nicht mehr viel ändern. Dies hat zweierlei Konsequenzen für Tracking betreibende Unternehmen, deren Geschäftsmodell auf die Erhebung von Nutzerdaten

gerichtet ist: Sie können einerseits damit beginnen, ihre eigenen Systeme und Maßnahmen mit den aktuellen Entwürfen der ePrivacy-Verordnung abzugleichen und darauf aufbauend neue Lösungswege zu erarbeiten. Andererseits müssen Tracking betreibende Unternehmen sich Gedanken darüber machen, wie sie ihre Geschäftsmodelle auch nach Inkrafttreten der Verordnung noch aufrechterhalten können.

4.3 Fazit und Positionierung

Tracking ist ein allgegenwärtiger Bestandteil des Internets. Eine Benutzung desselben, ohne selbst von Tracking betroffen zu sein, ist quasi unmöglich geworden. Dabei dient das Tracking nicht nur dazu, einfache Benutzerstatistiken von Webseiten zu erheben. Es ist gleichsam Teil einer mitunter sehr invasiven Überwachung, bei welcher sensible persönliche Daten gesammelt und verarbeitet werden. Tracking findet nahezu allgegenwärtig statt. Die mit Tracking verbundenen Risiken für Privatheit und informationelle Selbstbestimmung sind sehr kritisch zu sehen. Da im Zuge der ökonomisch getriebenen Vervielfältigung von Tracking-Instanzen gleichermaßen die Anzahl der Entitäten erhöht wird, welche Wissen über das Soziale erzeugen, stellt sich zudem die Frage nach der demokratischen Legitimation solcher Wissensproduzenten, sofern Wissen über das Soziale immer auch mit Intervention in das Soziale verbunden ist. Diese Kritik gilt es, trotz aller Chancen, die mit Trackingtechnologien verbunden sind, zu betonen, nicht zuletzt vor dem Hintergrund der Erkenntnis, dass Nutzer/-innen digitaler Medien Tracking-Verfahren als besorgniserregend und bedenklich erachten.

Jenseits des klassischen Trackings mit HTTP-Cookies ist in den letzten Jahren eine ganze Bandbreite an neuartigen Tracking-Verfahren entwickelt worden, welche überwiegend unbekannt sind. Gemeinsam ist den neuen Methoden, dass sie nicht nur äußerst intransparent, sondern darüber hinaus auch sehr schwer abzuwehren sind. Die Chancen, welche Trackingtechnologien besitzen, können sich aber nur dann entfalten, wenn ausreichende Schutzvorkehrungen getroffen werden und das Vertrauen der Nutzer/-innen in diese Anwendungen wiederhergestellt wird. Wünschenswert wäre, wenn Tracking gegenüber Nutzer/-innen klarer gekennzeichnet würde und es einfache Optionen für ein Opt-out, also für eine Deaktivierung, Beendigung oder graduelle Einschränkung des Trackings gäbe. Mit einem solchen Opt-out wie auch durch den Einsatz von separaten Tracking-Blockern dürfen keine Nachteile bei der Nutzung von Plattformen entstehen. Sollte aus Gründen der Nutzer/-innenfreundlichkeit dennoch ein Tracking erforderlich sein, so sind technische Maßnahmen zu ergreifen, dass dieses datenschutzfreundlich gestaltet ist. Neben den allgemeinen Regelungen der Datenschutz-Grundverordnung, welche auf das Tracking anwendbar sind, wäre es wünschenswert, insbesondere die Verwendung pseudonymisierter Nutzungsprofile zu privilegieren und den Do-not-track-Grundsatz gesetzlich zu verankern. Ferner wäre anzustreben, den Datenverarbeitungsvorgang nicht nur auf den Endgeräten der Nutzer/-innen zu regulieren, sondern den gesamten Datenverarbeitungsvorgangs des Trackings einheitlich zu regeln sowie ein abgestuftes Einwilligungssystem gesetzlich zu verankern, dass den Nutzer/-innen statt eines „take-it-or-leave-it"-Ansatzes echte Wahlmöglichkeiten lässt. Hervorzuheben ist, dass das Tracking auch deshalb so allgegenwärtig ist, weil darauf Geschäftsmodelle basieren. Die Nebenwirkung derselben sind mitunter massive Eingriffe in die Privatheit und informationelle Selbstbestimmung der Nutzer/-innen. Um dies zu verhindern, sind alternative Finanzierungsmodelle weiter auszubauen, bei denen auf ein Tracking verzichtet werden kann. Schließlich könnte auch darüber nachgedacht werden, inwiefern der mit Hilfe von Trackingmethoden erzeugte Wissenszugang sowie die daraus schöpfende Wissensproduktion selbst demokratisiert werden können, um die asymmetrischen Wissensverhältnisse zwischen Nutzer/-innen – also letztlich den Produzent/-innen der Daten – und Verarbeiter(inne)n auszugleichen. Hier stellt sich die Frage, ob Nutzer/-innen ein Mitbestimmungsrecht erhalten können. Das Ziel dieses Mitbestimmungsrechts sollte letztlich darin liegen, eine Situation herbeizuführen, in welcher das durch Tracking generierte Wissen nicht nur für die Interessen einiger We-

niger genutzt wird, sondern dem Allgemeinwohl dient und so das Potential moderner Trackingtechnologien zum Nutzen aller ausgeschöpft werden kann.

Anmerkungen

[1] Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., Diaz, C. (2014): The Web Never Forgets. Persistent Tracking Mechanisms in the Wild. In: Gail-Joon Ahn, Moti Yung und Ninghui Li (Hg.): *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14. ACM SIGSAC Conference*. Scottsdale, Arizona. New York: ACM Press, S. 674–689.

[2] van Eijk, N.; Helberger, N.; Kool, L.; van der Plas, A.; van der Sloot, B. (2012): Online tracking. Questioning the power of informed consent. In: *info* 14 (5), S. 57–73.

[3] Libert, T. (2015): Exposing the Hidden Web. An Aalysis of Third-Party HTTP Requests on 1 Million Websites. In: *International Journal of Communications* 9, S. 3544–3561.

[4] Andrejevic, M. (2002): The work of watching one another. Lateral surveillance, risk, and governance. In: *Surveillance & Society* 2 (4), S. 479–497.; Albrechtslund, A. (2008): Online social networking as participatory surveillance. In: *First Monday* 13 (3), S. 1–11.; Marwick, A. (2012): The Public Domain. Social Surveillance in Everyday Life. In: *Surveillance & Society* 9 (4), S. 378–393.

[5] Oostveen, A.-M., Vasalou, A, van den Besselaar, P., Brown, I. (2014): Child Location Tracking in the US and the UK. Same Technology, Different Social Implications. In: *Surveillance & Society* 12 (4), S. 581–593.

[6] Selke, S. (Hg.) (2016): Lifelogging. Digital self-tracking and Lifelogging - between disruptive technology and cultural transformation. Wiesbaden: Springer VS.

[7] Kühl, E. (2018): Der Feind in meinem Turnschuh. http://www.zeit.de/digital/datenschutz/2018-01/fitnesstracker-strava-soldaten-verrat-geheimnisse-fitnessapp-datenschutz/komplettansicht.

[8] Canossa, A. (2014): Reporting From the Snooping Trenches. Changes in Attitudes and Perceptions Towards Behavior Tracking in Digital Games. In: *Surveillance & Society* 12 (3), S. 433–436.; Hoffstadt, C., Nagenborg, M. (2009): Game Developers, Gods, and Surveillance. In: Luke Cuddy und John Nordlinger (Hg.): *World of Warcraft and Philosophy. Wrath of the Philosopher King*. Chicago, IL: Carus Publishing, S. 195–202.

[9] Brühl, J. (2017): So spioniert "Cayla" Kinder aus (Süddeutsche Zeitung). http://www.sueddeutsche.de/digital/verbotenes-spielzeug-so-spioniert-die-puppe-cayla-kinder-aus-1.3383387.

[10] Hern, A. (2017): Vibrator maker ordered to pay out C$4m for tracking users' sexual activity. https://www.theguardian.com/technology/2017/mar/14/we-vibe-vibrator-tracking-users-sexual-habits.

[11] Karaboga, M., Matzner T., Morlok T., Pittroff F., Nebel M., Ochs C., von Pape T., Pörschke J. V., Schütz P., & Fhom H. S.. (2015): Das versteckte Internet: zu Hause–im Auto–am Körper. White Paper. Schriftenreihe Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Eggenstein: Stober.

[12] Nissenbaum, H. (2010): Privacy in Context. Technology, Policy, and the Integrity of Social Life: Stanford University Press.; Rössler, B. (2001): Der Wert des Privaten. Frankfurt am Main: Suhrkamp.; Regan, P. M. (1995): Legislating Privacy. Technology, Social Values, and Public Policy. Chapel Hill: University of North Carolina Press.

[13] Matzner, T. (2016): Anonymität. In: Heesen, J. (Hg.): Handbuch Informations- und Medienethik. Stuttgart: Metzler, S. 248–254.

[14] Davis, J. L.; Jurgenson, N. (2014): Context collapse. Theorizing context collusions and collisions. In: Information, Communication & Society 17 (4), S. 476–485.

[15] BVerfGE 1983.

[16] Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y. et al. (2015): Digitale Demokratie statt Datendiktatur (Spektrum). http://www.spektrum.de/news/wie-algorithmen-und-big-data-unsere-zukunft-bestimmen/1375933?_druck=1.

[17] Foucault, M. (2006): Geschichte der Gouvernementalität 1: Sicherheit, Territorium, Bevölkerung: Vorlesung am Collège de France 1977/1978. 1. Aufl. Frankfurt am Main: Suhrkamp Verlag.

[18] Passoth, J. H.; Wehner, J. (2013): *Quoten, Kurven und Profile – Zur Vermessung der Sozialen Welt. Einleitung*, in ders. (Hg.), Quoten, Kurven und Profile, S. 7-17.

[19] Strum, S., Latour, B. (1987): Redefining the social link: from baboons to humans. In: *Social Science Information* 26(4), S. 783-802.

[20] Goffman, E. (1973): The Presentation of Self in Everyday Life. Woodstock, NY: Overlook Press.

[21] Garfinkel, H. (1984): Studies in Ethnomethodology. Cambridge: Polity.

[22] Lindemann, G. (2014): In der Matrix der digitalen Raumzeit. In: *Kursbuch 177: Privat 2.0*, S. 162-173.

[23] Kucklick, C. (2016): Die Granulare Gesellschaft. Wie das Digitale unsere Wirklichkeit auflöst. Berlin: Ullstein Verlag.

[24] Lindemann, G. (2014): In der Matrix der digitalen Raumzeit. In: *Kursbuch 177: Privat 2.0*, S. 162-173.: 167.

[25] Marres, N. (2017): Digital Sociology. The Reinvention of Social Research. Cambridge: Polity: 156; Thielmann, T. (2012): Taking into account: Harold Garfinkels Beitrag für eine Theorie sozialer Medien. In: *Zeitschrift für Medeinwissenschaft* 1/2012, S. 85-102.

[26] Latour, B., Jensen, P., Venturini, T., Grauwin, S., Bouillier, D. (2012): 'The whole is always smaller than its parts' - a digital test of Gabriel Tarde's monads. In: *The British Journal of Sociology* 63(4), S. 590-615.

[27] Latour, B. (2007): Beware, your imagination leaves digital traces. In: *Times Higher Literary Supplement (6. April 2007)*. http://www.bruno-latour.fr/sites/default/files/P-129-THES-GB.pdf.

[28] Ruppert, E., Law, J., Savage, M. (2013): Reassembling Social Science Methods: The Challenge of Digital Devices. In: *Theory, Culture & Society* 30(4), S. 22-46.

[29] Marres, N. (2017): Digital Sociology. The Reinvention of Social Research. Cambridge: Polity: 66.

Anmerkungen

[30] Marres, N. (2017): Digital Sociology. The Reinvention of Social Research. Cambridge: Polity: 61.

[31] In Alltagsgegenstände eingebettete Computer, die miteinander ggf. über das Internet vernetzt sind.

[32] Den interessierten Leser(inne)n sei an dieser Stelle auf frühere Veröffentlichungen des Forum Privatheit zum Thema verstecktes Tracking und Profilbildung im Kontext der Heimautomatisierung, von vernetzten Fahrzeugen und von tragbarer Datenverarbeitung (Wearable Computing) verwiesen (Karaboga et al. 2015; Ghiglieri et al. 2016). Weitere Studienpapiere (Eisele et al. 2017; Gassen & Fhom 2016) beschreiben WLAN-basierte Trackingmechanismen in öffentlichen Räumen, zum Beispiel in Einkaufsmeilen und Innenstädten.

[33] Kleine Computerprogramme, die in die Webseite eingebunden werden.

[34] Mayer, J. R. and Mitchell, J. C. (2012): Third-party web tracking. Policy and technology. In: *Security and Privacy (SP)*, IEEE Symposium on, S. 413–427. IEEE.

[35] Schneider, M., Enzmann, M., & Stopczynski, M. (2014): Web-tracking-report 2014. Fraunhofer-Verlag.

[36] Mayer J. R and Mitchell J. C. (2012): Third-party web tracking: Policy and technology. In: *Security and Privacy (SP)*, IEEE Symposium on, S. 413-427. IEEE.

[37] Roesner, F., Kohno, T., & Wetherall, D. (2012, 4): Detecting and defending against third-party tracking on the web. In: *Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation* (S. 12-12). USENIX Association.

[38] Kamkar, S. (2010, 9): Evercookie - virtually irrevocable persistent cookies. http://samy.pl/evercookie/.

[39] Soltani, A., Canty, S., Mayo, Q., Thomas, L., & Hoofnagle, C. J. (2010, 3): Flash Cookies and Privacy. In: *AAAI spring symposium: intelligent information privacy management* Vol. 2010, S. 158-163.

[40] Soltani, A., Canty, S., Mayo, Q., Thomas, L., & Hoofnagle, C. J. (2010, 3): Flash Cookies and Privacy. In *AAAI spring symposium: intelligent information privacy management* Vol. 2010, S. 158-163.

[41] lucb1e (2013): Cookieless cookies. http://lucb1e.com/rp/cookielesscookies/.

[42] Ayenson, M. D., Wambach, D. J., Soltani, A., Good, N., & Hoofnagle, C. J. (2011): Flash cookies and privacy II: Now with HTML5 and ETag respawning.

[43] Nikiforakis, N., Kapravelos, A., Joosen, W., Kruegel, C., Piessens, F., & Vigna, G. (2013, 5). Cookieless monster: Exploring the ecosystem of web-based device fingerprinting. In: *Security and privacy (SP), 2013 IEEE symposium on* Securtiy and Privacy. S. 541-555). IEEE.

[44] lucb1e (2013): Cookieless cookies. http://lucb1e.com/rp/cookielesscookies/.

[45] Mayer, J. R., & Mitchell, J. C. (2012, May). Third-party web tracking: Policy and technology. In: *Security and Privacy (SP), 2012 IEEE Symposium on Security and Privacy*. S. 413-427. IEEE.

Anmerkungen

[46] Eckersley, P. (2010, July). How unique is your web browser?. In: *Privacy Enhancing Technologies* Vol. 6205, S. 1-18.

[47] Boda, K., Földes, A., Gulyás, G., & Imre S. (2011): User tracking on the web via cross-browser fingerprinting. In: *Nordic Conference on Secure IT Systems*, S. 31–46. Springer.

[48] Eckersley, P. (2010, July). How unique is your web browser?. In Privacy Enhancing Technologies Vol. 6205, S. 1-18.

[49] Acar, G., Juarez, M., Nikiforakis, N., Diaz, C., Gürses, S., Piessens, F., & Preneel, B. (2013, November): FPDetective: dusting the web for fingerprinters. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* S. 1129-1140. ACM.

[50] Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014, November): The web never forgets: Persistent tracking mechanisms in the wild. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* S. 674-689. ACM.

[51] Englehardt, S. & Narayanan, A. (2016): Online tracking: A 1-million-site measurement and analysis. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM.

[52] Eckersley, P. (2010, July). How unique is your web browser?. In: *Privacy Enhancing Technologies* Vol. 6205, S. 1-18.

[53] Olejnik, Ł., Acar, G., Castelluccia, C., & Diaz, C. (2015, September). The leaking battery. In *International Workshop on Data Privacy Management* S. 254-263. Springer International Publishing.

[54] Brinkmann, M. (2016, 10): Mozilla cuts website access to Battery API in Firefox 52. https://www.ghacks.net/2016/10/31/mozilla-removes-battery-api-in-firefox-52/.

[55] Zeimpekis, V., Giaglis, G. M., & Lekakos, G. (2002): A taxonomy of indoor and outdoor positioning techniques for mobile location services. *ACM SIGecom Exchanges*, *3*(4), S. 19-27.

[56] Liu, H., Darabi, H., Banerjee, P., & Liu, J. (2007). Survey of wireless indoor positioning techniques and systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, *37*(6), S. 1067-1080.

[57] Han, J., Owusu, E., Nguyen, L. T., Perrig, A., & Zhang, J. (2012, January). Accomplice: Location inference using accelerometers on smartphones. In: *Communication Systems and Networks (COMSNETS), 2012 Fourth International Conference on Communication Systems and Networks.* S. 1-9. IEEE.

[58] Zhou, X., Demetriou, S., He, D., Naveed, M., Pan, X., Wang, X. & Nahrstedt, K. (2013, November). Identity, location, disease and more: Inferring your secrets from android public resources. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security.* S. 1017-1028. ACM.

[59] Do, T. M. T., & Gatica-Perez, D. (2014): The places of our lives: Visiting patterns and automatic labeling from longitudinal smartphone data. *IEEE Transactions on Mobile Computing*, *13*(3), S. 638-648.

Anmerkungen

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

[61] Gassen, M., & Fhom, H. S. (2016): Towards Privacy-preserving Mobile Location Analytics. In: EDBT/ICDT Workshops.

[62] Google. The New Multi-Screen World Understanding Cross-Platform Consumer Behavior. 2012. https://www.thinkwithgoogle.com/_qs/documents/871/multi-screen-world-infographic_infographics.pdf.

[63] tracking-part-1, November 2015.

[64] C. Calabrese et al. (2015, 10): Comments for november 2015 workshop on cross-device tracking, letter of the center for democracy & technology to the federal trade commission. https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf.

[65] Rouge P. Alva A. & Yeung C. Brookman, J. (2017): Cross-device tracking: Measurement and disclosures. . Proceedings on Privacy Enhancing Technologies, 2017(2), S. 133-148. https://www.degruyter.com/view/j/popets.2017.2017.issue-2/popets-2017-0020/popets-2017-0020.xml.

[66] Zimmeck, S., Li, J. S., Kim, H., Bellovin, S. M., & Jebara, T. (2017, August): A privacy analysis of cross-device tracking. In: 26th USENIX Security Symposium USENIX Security 17), S. 1391-1408. USENIX Association.

[67] Rouge P. Alva A. & Yeung C. Brookman, J. (2017): Cross-device tracking: Measurement and disclosures. Proceedings on Privacy Enhancing Technologies, 2017(2), S. 133-148. https://www.degruyter.com/view/j/popets.2017.2017.issue-2/popets-2017-0020/popets-2017-0020.xml.

[68] Rouge P. Alva A. & Yeung C. Brookman, J. (2017): Cross-device tracking: Measurement and disclosures. Proceedings on Privacy Enhancing Technologies, 2017(2), S. 133-148. https://www.degruyter.com/view/j/popets.2017.2017.issue-2/popets-2017-0020/popets-2017-0020.xml.

[69] Arp, D., Quiring, E., Wressnegger, C., & Rieck, K. (2017, 4): Privacy threats through ultrasonic side channels on mobile devices. In: *Security and Privacy (EuroS&P)*, 2017 IEEE European Symposium on Security and Privacy. S. 35-47. IEEE.

[70] Mavroudis, V., Hao, S., Fratantonio, Y., Maggi, F., Kruegel, C., & Vigna, G. (2017): On the Privacy and Security of the Ultrasound Ecosystem. Proceedings on Privacy Enhancing Technologies, 2017(2), S. 95-112.

[71] Arp, D., Quiring, E., Wressnegger, C., & Rieck, K. (2017, 4). Privacy threats through ultrasonic side channels on mobile devices. In Security and Privacy (EuroS&P), 2017 IEEE European Symposium on Security and Privacy. S. 35-47. IEEE.

[72] Mavroudis, V., Hao, S., Fratantonio, Y., Maggi, F., Kruegel, C., & Vigna, G. (2017): On the Privacy and Security of the Ultrasound Ecosystem. Proceedings on Privacy Enhancing Technologies, 2017(2), S. 95-112.

[73] Zimmeck, S., Li, J. S., Kim, H., Bellovin, S. M., & Jebara, T. (2017, 4): A privacy analysis of cross-device tracking. In 26th USENIX Security Symposium USENIX Security. S. 1391-1408. USENIX Association.

[74] C. Calabrese et al. (2015, 10): Comments for november 2015 workshop on cross-device tracking, letter of the center for democracy & technology to the federal trade commission. https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf.

[75] Arp, D., Quiring, E., Wressnegger, C., & Rieck, K. (2017, 4): Privacy threats through ultrasonic side channels on mobile devices. In: *Security and Privacy (EuroS&P)*, 2017 IEEE European Symposium on Security and Privacy. S. 35-47. IEEE.

[76] (2016, 3): FTC Issues Warning Letters to App Developers Using 'Silverpush' Code. https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code.

[77] (2013, 10): Future of Privacy Forum. Mobile Location Analytics Code of Conduct. Technical report, Future of Privacy Forum.

[78] Gassen, M. & Simo Fhom, H. (2016): Towards Privacy-preserving Mobile Location Analytics. EDBT/ICDT Workshops.

[79] Lohmann, M. (2017): Marketingmonitor Handel 2016 – 2019 - Studien, Datenbanken und Fachmagazine für den Handel. Retrieved from https://de.statista.com/statistik/daten/studie/630836/umfrage/entwicklung-der-bruttowerbeaufwendungen-im-online-marketing-in-deutschland/.

[80] Hess, T., & Schreiner, M. (2012): Ökonomie der Privatsphäre - Eine Annäherung aus drei Perspektiven. Datenschutz und Datensicherheit, 36(2), S. 105-109.

[81] Lambrecht, A., & Tucker, C. (2013): When Does Retargeting Work? Information Specificity in Online Advertising. Journal of Marketing Research, 50(5), S. 561-576.

[82] Budak, C., Goel, S., Rao, J. M., & Zervas, G. (2014): Do-not-track and the economics of third-party advertising. Boston University School of Management Research Paper Series No. 2505643.

[83] Cecere, G., Le Guel, F., Manant, M., & Soulié, N. (2017): The Economics of Privacy. In S. Durlauf & L. E. Blume (Hg.), The New Palgrave Dictionary of Economics. Vol. 1, S. 1-11. Basingstoke: Palgrave Macmillan.

[84] Rayna, T., Darlington, J., & Striukova, L. (2015): Pricing music using personal data: mutually advantageous first-degree price discrimination. Electronic Markets, 25 (2), S. 139-154.

[85] Morlok, T., Matt, C., & Hess, T. (2017): Privatheitsforschung in den Wirtschaftswissenschaften: Entwicklung, Stand und Perspektiven. Retrieved from https://EconPapers.repec.org/RePEc:zbw:lmuwim:12017.

[86] Rayna, T., Darlington, J., & Striukova, L. (2015): Pricing music using personal data: mutually advantageous first-degree price discrimination. Electronic Markets, 25(2), S. 139-154.

[87] Lyon, D. (2003): Surveillance as social sorting. Computer codes and mobile bodies. In: David Lyon (Hg.): Surveillance as Social Sorting. Privacy, risk, and digital discrimination. London: Routledge, S. 13–30.

[88] O'Neil, C. (2016): Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy. New York: Crown Publishers; Schaar, P. (2016): Algorithmentransparenz. In: Dix, A., Franßen G., Kloepfer, M., Schaar, P., Schoch, F. &

Voßhoff, A. (Hg.): Informationsfreiheit und Informationsrecht. Jahrbuch 2015. Berlin: Lexxion Verlagsgesellschaft, S. 23–36; Pasquale, F. (2015): The Black Box Society. The Sectret Algorithms That Control Money and Information. Cambridge, Massachusetts: Harvard University Press.

[89] Lanier, J. (2013): Who Owns the Future? New York: Simon & Schuster.

[90] Masur, P. K., Teutsch, D., Dienlin, T., & Trepte, S. (2017). Online-Privatheitskompetenz und deren Bedeutung für demokratische Gesellschaften. Forschungsjournal Soziale Bewegungen, 30(2), 180-189.

[91] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. EU vom 4. Mai 2016, L 119, 1.

[92] Die nachfolgenden Ausführungen zur ePrivacy-VO-E beziehen sich alle auf den Entwurf des Europäischen Parlaments, s. Legislativbericht v. 23. Oktober 2017, A8-0324/2017. Nach Art. 29 Abs. 2 ePrivacy-VO des Kommissionsentwurfes (s. KOM(2017) 10 endg.) sollte sie ursprünglich ab dem 25. Mai 2018 gelten, wird aber frühestens 2019 in Kraft treten.

[93] Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 28. September 2017 (BGBl. I S. 3530) geändert worden ist.

[94] Diese Auffassung ist indes umstritten, da im Gegensatz zu § 15 Abs.3 TMG (Opt-out) die RL 2002/58/EG in Art. 5 Abs. 3 eine vorherige Einwilligung des Nutzers vorschreibt (Opt-in); siehe dazu Geminn/Richter, in: Roßnagel, Das neue Datenschutzrecht, 2018, § 8 Rn. 152.

[95] Kremer, in: Auer-Reinsdorff/Conrad, Handbuch IT-und Datenschutzrecht, 2. Auflage 2016, Teil D, Rn. 65.

[96] Dazu z. B. Jandt/Schaar/Schulz, in: Roßnagel, Recht der Telemediendienste, 2013, § 13 TMG, Rn. 51 ff.

[97] Geminn/Richter, in: Roßnagel, Europäische Datenschutz-Grundverordnung, 2017, § 4 Rn. 295; Geminn/Richter, in Roßnagel, Das neue Datenschutzrecht, 2018, § 8 Rn. 153; Grigorjew, in Roßnagel, Das neue Datenschutzrecht, 2018, § 8 Rn. 216.

[98] Siehe dazu Geminn/Richter, in: Roßnagel, Das neue Datenschutzrecht, 2018, § 8 Rn. 130 f., 140.

[99] Bundesnetzagentur, ABl.4/2015, 1140; Mantz/Sassenberg, NJW 2014, 3537 (3538).

[100] Siehe dazu Geminn/Richter, in: Roßnagel, Das neue Datenschutzrecht, 2018, § 8 Rn. 68.

[101] Bock, Beck´scher TKG-Kommentar 2013, § 88 Rn. 15.

[102] Oberthür, in: Kramer, IT-Arbeitsrecht, 2017, Rn. 462.

[103] Bock, in: Geppert/Schütz 2013, TKG Kommentar, 2013, § 88 Rn. 11.

[104] Braun, in: Geppert/Schütz 2013, TKG Kommentar, 2013, § 91 Rn. 12; Klesczewski, in: Säcker, TKG Kommentar, 2013, § 91 Rn. 30.

[105] Braun, in: Geppert/Schütz 2013, TKG Kommentar, 2013, § 91 Rn. 12.

[106] Vgl. die Ausführungen zu § 3 Nr. 6 TKG.

[107] Zur Ablösung der RL 2002/58/EG durch ePrivacy-VO siehe Punkt 3.4.4.

[108] Siehe dazu Ausführungen Punkt 3.4.2.

[109] Neben Art. 4 Nr. 4 DSGVO auch z.B. in Erwägungsgrund 60, 63, 70 bis 72; Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g, Art. 15 Abs. 1 lit. h DSGVO.

[110] Zur Abwägung betroffener Interessen Grigorjew, in: Roßnagel, Das neue Datenschutzrecht, 2018, § 8 Rn. 164 ff.

[111] So auch Schleipfer, ZD 2017, 460 (462).

[112] Drewes, CR 2016, 721 (725 f.); vgl. auch Richter, in: Roßnagel, Das neue Datenschutzrecht 2018, § 7 184.

[113] Pseudonyme Nutzungsprofile werden nicht durch nachträgliche Pseudonymisierung gebildet; diese sind von Anfang an pseudonym zu erstellen, s. Schleipfer, ZD 2015, 399 (401); ders., ZD 2017, 460 (463).

[114] Wirken die pseudonymisierten Daten für den Verantwortlichen wie anonyme Daten, unterfallen sie nicht der Datenschutz-Grundverordnung.

[115] In Erwägungsgrund 85 ist zudem die Rede von "unbefugter Aufhebung der Pseudonymisierung".

[116] Siehe dazu http://www.horizont.net/marketing/nachrichten/Datenschutz-Die-E-Privacy-Verordnung-kommt-spaeter-162887.

[117] S. Fn. 50.

[118] S. Fn. 50.

[119] S. Roßnagel, Medienwirtschaft, 1/2018 i.E.

[120] Siehe dazu Roßnagel, in: ders., Das neue Datenschutzrecht, 2018, § 1 Rn. 46; Husemann, in Roßnagel, Das neue Datenschutzrecht, 2018, § 3 Rn. 19 ff.

[121] Nach Art. 4 Abs. 3 lit. c ePrivacy-VO-E sind Inhaltsdaten die Inhalte, die mittels elektronischer Kommunikationsdienste übermittelt werden, also das Gespräch oder der Inhalt einer E-Mail oder Textnachricht.

[122] Gemäß Art. 4 Abs. 1 lit. c ePrivacy-VO-E sind Metadaten (auch ,,Verkehrsdaten") die Daten, die in einem elektronischen Kommunikationsnetz zu Zwecken der Übermittlung einer Kommunikation verarbeitet werden, wie z. B. die Telefonnummer, die Absender und Empfänger von Textnachrichten oder E-Mails, Datum und Uhrzeit usw.

[123] Der Begriff der Endeinrichtung ist gemäß Art. 4 Abs. 1 lit. c ePrivacy-VO-E gleich dem in Art. 1 Nr. 1 RL 2008/63/EG der Kommission v. 20.06.2008 über den Wettbewerb auf dem Markt für Telekommunikationsendeinrichtungen, ABl. EU 2008, Nr. L 162, 20.

Anmerkungen

[124] Erwägungsgrund 22 ePrivacy-VO-E.

[125] Legislativbericht v. 23.10.2017, Amendment 25, S. 26.

[126] S. Roßnagel, Medienwirtschaft, 1/2018 i.E.

[127] Herbrich, T., Der Vorschlag für eine ePrivacy-Verordnung-EU (Teil 2), jurisPR-ITR 23/2017 Anm. 2.

[128] Roßnagel, Medienwirtschaft, 1/2018 i.E; Lurtz, ZD-aktuell 2017, 05707.

[129] Bitkom, E-Privacy Verordnung gefährdet digitale Innovationen v. 19.10.2017, https://www.bitkom.org/Presse/Presseinformation/E-Privacy-Verordnung-gefaehrdet-digitale-Innovationen.html.

[130] Heise online, Verlage befürchten massive Auswirkungen durch e-Privacy-Verordnung v. 29.1.2018, https://heise.de/-3953161.

[131] European Data Protection Supervisor, Opinion 6/2017, S. 28 f.

[132] Art.-29-Datenschutzgruppe, WP 247 vom 4. April 2017.

[133] Merzdovnik, G., Huber, M., Buhov, D., Nikiforakis, N., Neuner, S., Schmiedecker, M., & Weippl, E. (2017, 4). Block me if you can: A large-scale study of tracker-blocking tools. In Security and Privacy (EuroS&P), 2017 IEEE European Symposium on Security and Privacy. S. 319-333. IEEE.

[134] Merzdovnik, G., Huber, M., Buhov, D., Nikiforakis, N., Neuner, S., Schmiedecker, M., & Weippl, E. (2017, April). Block me if you can: A large-scale study of tracker-blocking tools. In: *Security and Privacy (EuroS&P),* 2017 IEEE European Symposium on Security and Privacy. S. 319-333. IEEE.

[135] AdAway: https://adaway.org/.

[136] Pi-hole: A black hole for internet advertisements. https://pi-hole.net/.

[137] Bokhorst, M. (2017): Xprivacy-the ultimate, yet easy to use, privacy manager.

[138] Chitkara, S., Gothoskar, N., Harish, S., Hong, J. I., & Agarwal Y. (2017): Does this app really need my location? Context-aware privacy management for smartphones. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, Vol. 1, No. 3, Art. 42, 22 Seiten.

[139] Eg. 23 COM(2017) 10 final.

Weitere Veröffentlichungen in der Reihe „White Paper“

Anmerkungen

Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt:

Murat Karaboga / Philipp Masur / Tobias Matzner / Cornelia Mothes / Maxi Nebel / Carsten Ochs / Philip Schütz / Hervais Simo Fhom

White Paper

Selbstdatenschutz

2. Auflage, November 2014

Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt:

Murat Karaboga / Tobias Matzner / Tina Morlok / Fabian Pittroff / Maxi Nebel / Carsten Ochs / Thilo von Pape / Julia Victoria Pörschke / Philip Schütz / Hervais Simo Fhom

White Paper

Das versteckte Internet

Zu Hause - Im Auto - Am Körper

1. Auflage, Juli 2015

Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt:

Morlok, Tina / Matt, Christian / Hess, Thomas

White Paper

Privatheit und Datenflut in der neuen Arbeitswelt

Chancen und Risiken einer erhöhten Transparenz

1. Auflage, Dezember 2015

Anmerkungen

Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt:

Michael Friedewald / Hannah Obersteller / Maxi Nebel / Felix Bieker / Martin Rost

White Paper

Datenschutz-Folgenabschätzung

Ein Werkzeug für einen besseren Datenschutz

2. Auflage, Mai 2016

Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt:

Daniel Eisele / Olga Grigorjew / Murat Karaboga / Tobias Matzner / Tina Morlok / Maxi Nebel / Carsten Ochs / Rasmus Robrahn / Christine Rzepka / Hervais Simo Fhom

White Paper

Privatheit in öffentlichen WLANs

Spannungsverhältnisse zwischen gesellschaftlicher Verantwortung, ökonomischen Interessen und rechtlichen Anforderungen

1. Auflage, März 2017

IMPRESSUM

Presse und Kommunikation:
Barbara Ferrarese, M.A.
Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

Telefon +49 721 6809-678
E-Mail presse@forum-privatheit.de

Projektkoordination:
Michael Friedewald
Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

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

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
Mai 2018

Zitiervorschlag:
Ammicht Quinn et al. (2018): White Paper Tracking. Beschreibung und Bewertung neuer Methoden. Hrsg.: Michael Friedewald et al., Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Karlsruhe: Fraunhofer ISI.

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 DUISBURG ESSEN
Offen im Denken

EBERHARD KARLS UNIVERSITÄT TÜBINGEN
INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein