Kompetenzzentrum
Öffentliche IT

KOMPETENZZENTRUM ÖFFENTLICHE INFORMATIONSTECHNOLOGIE

INTERNETTRACKING

Gabriele Goldacker

Gefördert durch:
Bundesministerium des Innern, für Bau und Heimat
Fraunhofer FOKUS

IMPRESSUM

Autoren:
Gabriele Goldacker

Gestaltung:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

ISBN: 978-3-9818892-6-0

1. Auflage September 2018

Bildnachweise:

Seite 1: sonnenstern
https://pixabay.com/de/hund-schnee-jagen-gestr%C3%BCpp-1174432/
Seite 6: darkmoon1968
https://pixabay.com/de/katze-mieze-glas-lustig-neugierig-2665646/
Seite 11: coffy
https://pixabay.com/de/hund-schn%C3%BCffeln-suchen-schwanz-142328/
Seite 17: Pezibear
https://pixabay.com/de/hund-malteser-junghund-wei%C3%9F-klein-1143500/
Seite 18: ulleo
https://pixabay.com/de/hund-mischling-tier-haustier-1784278/
Seite 20: kiragrafie
https://pixabay.com/de/schweine-schlamm-matsch-schweinchen-1463821/
Seite 25: jarekgrafik
https://pixabay.com/de/fuchs-tier-r%C3%A4uber-slowakei-tatry-1419362/
Seite 28: Counselling
https://pixabay.com/de/hund-welpe-jack-russell-chihuahua-2086403/
Seite 32: schuetz-mediendesign
https://pixabay.com/de/b%C3%A4r-braunb%C3%A4r-ursus-arctos-tier-1606953/
Seite 38: Pixel-mixer
https://pixabay.com/de/wolf-predator-raubtier-1583199/

VORWORT

Die offensichtlichen Ergebnisse von Internettracking – auf die eigene Person zugeschnittene Onlinewerbung, Suchmaschinenergebnisse und Vorschläge von Video- und Audioplattformen – beängstigen viele Nutzer[1]. Sie übertragen Erfahrungen aus dem nicht digitalen Leben und empfinden es als unangenehm, dass große (und kleine) Unternehmen so viel und so persönliches Wissen über sie besitzen, obwohl sie zu ihnen nur eine unverbindliche oder gar keine direkte Beziehung haben.

Einerseits sind diese Gefühle rational oft unbegründet, da sich viele Unternehmen, die Internettracking für Werbezwecke oder passgenauere Online-Dienstleistungen nutzen, nicht für den konkreten Menschen hinter einem bestimmten Satz qualitativer und quantitativer Eigenschaften interessieren. Sie kategorisieren ihn lediglich anhand dieser Eigenschaften und sprechen ihn später einfach wie jedes x-beliebige andere Mitglied dieser Kategorien an. Passen die Kategorien, dann können relevante Werbung und angepasste Dienstleistungen das Nutzungserlebnis durchaus positiver gestalten.

Andererseits greift Internettracking – insbesondere wenn es ohne Zustimmung des Nutzers oder in einer von ihm nicht überblickten Breite oder Tiefe erfolgt – deutlich in die informationelle Selbstbestimmung ein und bedarf schon allein deshalb einer gesellschaftlichen Positionsbestimmung. Zudem gewinnen durch Internettracking erfasste Daten zunehmend das Interesse von Versicherungsunternehmen, Kreditinstituten und Scoring-Agenturen – ganz abgesehen von Ermittlungsbehörden und Geheimdiensten –und können sich über diesen Weg nachteilig für die Betroffenen auswirken. Nicht zu vergessen ist, dass auch die organisierte Kriminalität, beispielsweise in den Bereichen Einbruch oder Erpressung, Nutzen aus Trackingdaten ziehen kann.

Veränderte politische Verhältnisse könnten dazu führen, dass Trackingdaten an staatliche Stellen herausgegeben werden müssen und so – auch weit im Nachhinein – beispielsweise zur Identifikation regierungskritischer Menschen genutzt werden können.

In diesem White Paper zeigen wir auf, welche Daten durch Tracking gewonnen und wie Nutzer wiedererkannt werden. Wir identifizieren und bewerten die Chancen und Risiken von Internettracking und leiten daraus Handlungsempfehlungen für die öffentliche Hand ab.

Ihr Kompetenzzentrum Öffentliche IT

[1] Wenn wir in diesem Dokument von Menschen als Nutzern, Bürgern usw. reden, sind damit stets Personen jedweden Geschlechts gemeint.

INTERNETTRACKING GEFÄHRDET
DIE FREIE MEINUNGSBILDUNG.

INHALTSVERZEICHNIS

1. THESEN

Internettracking gefährdet die Informationsfreiheit[2], die anonyme freie Meinungsäußerung, Whistleblowing und die freie Meinungsbildung.

Erfasste Daten können auch lange im Nachhinein genutzt werden, um konkrete Menschen zu identifizieren und zu lokalisieren. Die Angst vor den unbekannten zukünftigen Bewertungsmaßstäben und ihren Folgen erzeugt Konformitätszwang. Inhaltsangebote und Werbung, die auf Basis von Tracking individualisiert sind, schaffen Filterblasen und beeinträchtigen so die wohlinformierte persönliche Meinungsbildung.

Internettracking schafft lohnende Angriffspunkte für Ausspähung und Identitätsdiebstahl durch Dritte..

Bei unqualifizierter oder unsensibler Gestaltung von Webseiten und E-Mails ist eine (unnötige) Weitergabe personenbezogener Daten sehr wahrscheinlich, da z. B. Filterung oder Pseudonymisierung zusätzlichen Aufwand erfordern. Die Konzentration der Daten vieler getrackter Individuen bei global agierenden Trackingdiensten macht diese Dienste zu lohnenden Angriffszielen, wobei die häufig unverschlüsselte Kommunikation zudem Angriffe erleichtert.

Internettracking lässt sich technisch nicht umfassend und dauerhaft verhindern.

Manche Maßnahmen gegen Internettracking führen zu Funktions- oder erheblichen Komforteinbußen. Die Neu- und Weiterentwicklung von Trackingmethoden findet so rasant statt, dass die Betroffenen viele eingesetzte Methoden oft noch nicht einmal grundsätzlich kennen und etablierte Gegenmaßnahmen schnell ins Leere laufen können.

Die Nutzungsmöglichkeiten sowie die individuellen und gesellschaftlichen Auswirkungen durch Internettracking gewonnener Daten beginnen erst, sich zu zeigen.

Immer detailliertere und umfangreichere Datensammlungen bezüglich der getrackten Individuen besitzen nicht nur für das Bewerben von Waren und Dienstleistungen einen Nutzwert, sondern auch z. B. für Versicherer, politische Organisationen, Ermittlungsbehörden, Geheimdienste und sogar für Kriminelle. Höhere Versicherungsprämien für Risikofreudige oder höhere Preise für Gutverdiener sind nicht das Ende möglicher Auswirkungen.

Werden Trackingdaten ohne Berücksichtigung des Kontextes ausgewertet, kann selbst positives Verhalten der Betroffenen negative Auswirkungen für sie haben.

Werden z. B. bei der Bewertung gesundheitsbewussten oder risikoarmen Verhaltens aktuelle Maßstäbe auf zurückliegendes Verhalten angewendet, kann damals vermeintlich positives Verhalten zu einer negativen Bewertung führen.

Das Datenschutzrecht bietet keinen wirksamen prohibitiven Schutz.

In der Praxis lassen sich viele Websites umfängliche Rechte zur Datenerfassung und -verarbeitung einräumen (breit gefasster Verwendungszweck, der nahezu unbegrenzte Aufbewahrung ermöglicht). Die Nutzer stimmen meist zu. Oft sind sie mit den Geschäftsbedingungen und Datenschutzerklärungen der Anbieter überfordert oder befürchten funktionelle Einschränkungen bei Nichtzustimmung, was sich derzeit z. B. beim Cookie-Gebrauch häufig bestätigt.

Auskunfts-, Berichtigungs- und Löschungsrechte laufen beim Internettracking ins Leere.

Ein Großteil der Trackingdienste agiert für die Nutzer unsichtbar. Ihre Aktivitäten und Identitäten sind nur durch die Analyse von komplexem und verschachteltem Webseitencode feststellbar, was Nutzer in der Regel überfordert.

Es gibt sinnvolle Anwendungsfälle für Internettracking.

Die Auswertung der Nutzung einer Website durch eine bestimmte Person kann zu einem besseren Nutzungserlebnis führen, wenn daraufhin z. B. bereits bekannte Inhalte ausgeblendet werden oder die Ergonomie von Webseiten erhöht wird. Geotracking kann bei gesundheitlichen Problemen oder einem Unfall die Lokalisation der betroffenen Person wesentlich vereinfachen.

[2] Im Glossar enthaltene Begriffe sind bei erstmaliger Erwähnung durch »▸« gekennzeichnet.

2. WAS IST INTERNETTRACKING?

2.1 DEFINITION

Internettracking ist jede Form der auf einen einzelnen Nutzer bezogenen Aufzeichnung oder Verarbeitung von Verlaufs-, Verhaltens-, Zustands- oder Inhaltsdaten▸, die bei der Nutzung des Internets anfallen oder gezielt für Trackingzwecke erzeugt werden und die nicht ausschließlich der direkten Erbringung einer angeforderten Online-Dienstleistung für diesen Nutzer dient.[3]

Eine solche Definition besitzt naturgemäß Unschärfen, z. B. hier bei der Frage, ob die Wiederaufnahme eines Onlinekurses nach Monaten der Untätigkeit durch den Nutzer noch die Fortsetzung derselben Dienstleistung darstellt. Im Kern wird man aber von einem gemeinsamen Verständnis dieser Definition ausgehen können.

2.2 WARUM INTERNETTRACKING?

Internettracking dient heute in erster Linie der Optimierung von Werbeeinblendungen (»individualisierte Werbung«▸) bei Online-Diensten▸, insbesondere, um Dienste zu finanzieren, bei denen die Nutzer keine finanzielle Gegenleistung erbringen müssen und sich die Anbieter auch nicht unmittelbar über den Verkauf, die Vermietung oder die Vermittlung von Waren oder Dienstleistungen an die Nutzer finanzieren[4]. Fremdwerbung ist derzeit für viele Online-Dienste die einzige oder die hauptsächliche Einnahmequelle. Eine repräsentative Umfrage des Kompetenzzentrums Öffentliche IT im Dezember 2017 hat z. B. gezeigt, dass die Mehrheit der Antwortenden nicht bereit ist, für werbefreie alternative Online-Plattformen zu bezahlen. Möglichst viel Erfolg versprechende Werbeeinblendungen sind in diesem Kontext ein Mittel, die Interessen aller Beteiligten – Online-Anbieter▸ (z. B. Websites), Werbetreibende und Nutzer – gegeneinander auszubalancieren.

Zu dieser verbreitetsten Ausprägung des Trackings gehören zwei große Teilbereiche: die Bildung von Nutzerprofilen und die Beobachtung der Wirksamkeit von Werbung, die auf Webseiten Dritter angezeigt wird. Die Profilbildung dient der Gewinnung von Daten, anhand derer möglichst viel Erfolg versprechende Werbung und der optimale Werbungskontext (z. B. Tageszeit, Wochentag …) ausgewählt werden können. Ermittelt (bzw. tlw. auch beim Nutzer abgefragt) werden z. B. (werberelevante) Eigenschaften, Vorlieben, Verhaltensmuster und Kontakte zu Personen und Institutionen. Die Wirksamkeitsbeobachtung zeichnet profilbezogen auf, welche Wirkung eine konkrete Werbemaßnahme – eine Einzelwerbung oder eine Kombination mehrerer Werbemittel – tatsächlich erzielt. Typisch beim werbungsbezogenen Tracking ist, dass die anfallenden Verlaufs-, Verhaltens- und Inhaltsdaten – die Tracking-Quelldaten – von einem, meist sogar von mehreren Trackingdiensten aufgezeichnet und verarbeitet werden, mit denen der Nutzer nicht direkt in Kontakt steht.

Ein weiterer Teil des Trackings erfolgt (zumindest vordergründig), um den getrackten Online-Dienst zu verbessern, also beispielsweise, um ergonomische Schwachstellen auf Webseiten zu erkennen oder um das eigentliche Dienstleistungs-/Warensortiment bzw. dessen Präsentation zu optimieren. Eine spezielle Ausprägung dabei ist die individualisierte Optimierung der angezeigten Suchergebnisse und ihrer Reihenfolge bei Suchmaschinen und der präsentierten Nachrichten und deren Reihenfolge z. B. in sozialen Netzen. Ähnlich sind auch eigenwerbliche Elemente auf Webseiten (»andere Kunden kauften auch …«, »das könnte Sie auch interessieren …«) einzuordnen. In all diesen Optimierungsfällen ist der Anbieter des Online-Dienstes jeweils gleichzeitig Nutzer der durch Tracking gewonnenen Daten.

Ein nicht unerheblicher Teil des Trackings wird offenbar »auf Vorrat« durchgeführt, ohne dass die das Tracking auslösende oder die aufzeichnende Stelle klare Vorstellungen hat, wozu die erfassten Daten verwendet werden sollen. Es darf auch angenommen werden, dass – nachdem sich der wirtschaftliche Wert umfänglichen, individuellen Trackings gezeigt hat – Unternehmen Daten aufzeichnen und (vor-)verarbeiten, um sie anschließend weiterzuveräußern.[5]

[3] Im Folgenden wird verkürzend oft nur von Tracking und Trackingdaten gesprochen. Damit sind hier stets Internettracking und auf der Basis von Internettracking gewonnene Daten gemeint.

[4] Es gibt auch Händler und Dienstleister, die auf ihren Webseiten zusätzlich Waren/Dienstleistungen anderer (nicht konkurrierender) Unternehmen bewerben (lassen).

[5] Bekannt ist beispielsweise, dass Internetanbieter ortsbezogene Daten zur Internetnutzung vermarkten.

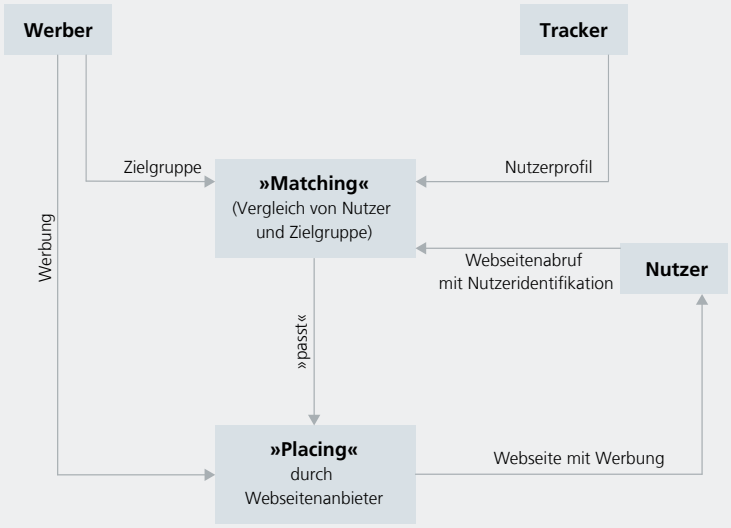

Abbildung 1: Rollen im Tracking-Ökosystem (vereinfacht)

Neben diesen im weitesten Sinne wirtschaftlich veranlassten Formen des Trackings werden Trackingdaten zunehmend für die Auswahl individualisierter politischer Botschaften verwendet (wozu allerdings derzeit noch vorwiegend ursprünglich unter Werbegesichtspunkten gesammelte Trackingdaten genutzt werden). Tracking dient auch der Erkennung von Angriffen auf die IT-Systeme von Online-Anbietern, wozu allerdings keine detaillierten Profildaten erforderlich sind. Zudem findet Tracking direkt durch Ermittlungsbehörden und Geheimdienste statt, außerdem wird es zum Zweck der Industriespionage und weiterer rechtswidriger Tätigkeiten genutzt. Auf diese Formen wird allerdings im Weiteren nur am Rande eingegangen.

2.3 VORGANGSBEDINGTE DATENVERARBEITUNG

Vom Internettracking nicht immer leicht zu trennen ist die vorgangsbedingte Datenerfassung und -verarbeitung, da in beiden Fällen dieselben Mittel und Methoden zum Einsatz kommen. Um vorgangsbedingte Datenverarbeitung handelt es sich zum Beispiel, wenn während eines Einkaufvorganges der Inhalt eines virtuellen Warenkorbes aufbewahrt wird oder während einer Domänensitzung‣ die Zugriffsrechte auf bestimmte Online-Inhalte anhand eines während einer initialen Authentifizierung vergebenen Kennzeichens ermittelt werden. Die Daten müssen dabei für den Vorgang notwendig und angemessen sein. Nach Abschluss des Vorgangs werden alle vorgangsbedingten Daten auf dem Gerät des Nutzers gelöscht, beim Online-Anbieter werden lediglich gegebenenfalls Ergebnisdaten (z. B. die konkrete Bestellung) gespeichert und die Daten werden weder Trackingdienstleistern zur Verfügung gestellt noch mit Daten anderer Online-Anbieter abgeglichen. Die Dauer eines solche Vorgangs sollte den typischen Nutzererwartungen entsprechen, verlässt dieser beispielsweise eine Website, ohne die Waren im Warenkorb gekauft zu haben, sollte der Warenkorb gelöscht oder er gefragt werden, ob der Warenkorb für die nächste Sitzung aufbewahrt werden soll.

2.4 DER TRACKINGBASIERTE WERBUNGSKREISLAUF IM INTERNET

Wie bereits in Abschnitt 2.2 erwähnt, wird Tracking in mehreren Phasen des Nutzerkontaktes eingesetzt. Logisch am Anfang steht das Tracking zum Zweck der Profilbildung. Dieses Tracking erfolgt allerdings fortlaufend, um das Profil aktuell zu halten und es möglichst mit immer weiteren Details anzureichern.

Die Profile der einzelnen Nutzer werden sogenannten Personas‣ – modellhaften Profilen, die mit bestimmten Werbestichwörtern verknüpft sind – zugeordnet, um beim Auftreten einer Werbegelegenheit beim Nutzer innerhalb von Millisekunden gut geeignete Werbung (»Targeting«‣) bestimmen zu können. Mit fortschreitenden technischen Möglichkeiten und verbesserten Werbungsauswahlprozessen kann der Detailgrad der Personas und damit deren Zahl nach wie vor gesteigert werden. Wurde etwa ursprünglich nur danach gruppiert, ob ein Nutzer generell sportaffin ist oder nicht, können heute Sportarten, aktives bzw. passives Interesse, Altersgruppen, die Bevorzugung bestimmter Sportartikelhersteller usw. berücksichtigt werden. Während thematisch unter einem Oberthema angesiedelte, konkretere Personas eine passgenauere Werbungsauswahl aus einem Kreis verwandter Werbender ermöglichen, eröffnen themenübergreifende Personas auch eine entsprechende Werbungsauswahl: Für Personas, die die Anhänger von Computerspielen zu einer bestimmten Sportart modellieren, kann sowohl Werbung in Bezug auf die Sportart selbst als auch für Computerspiele zu ähnlichen Sportarten geeignet sein. Mit dem (möglichen) Detailgrad der Personas steigt wiederum das Interesse an noch detaillierteren Nutzerprofilen.

Wurde eine geeignete Werbung platziert, besteht natürlich auch ein Interesse daran, wie der Nutzer auf diese reagiert, weshalb die Reaktionen möglichst ebenfalls getrackt werden. Zum einen bestimmen sich die Einnahmen des die Werbung

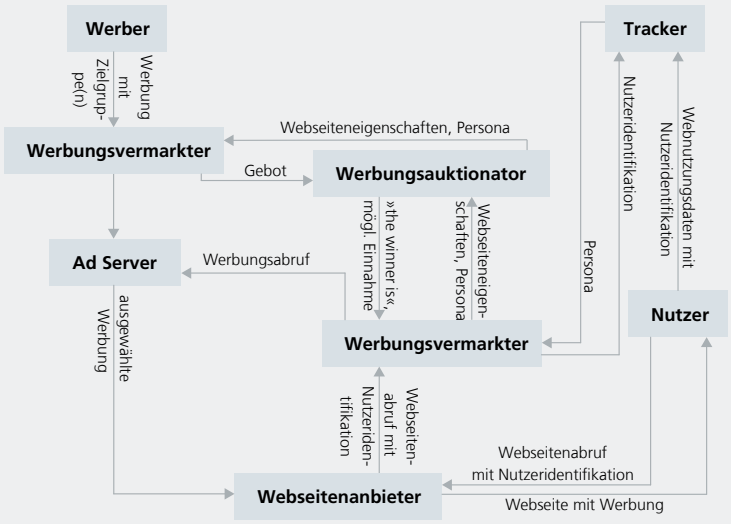

Abbildung 2: Akteure im Tracking-Ökosystem

auswählenden Unternehmens bei bestimmten Geschäftsmodellen direkt aus den Werbeanzeigen, die zumindest angeklickt wurden (»Pay per Click«), zum anderen sind Klickraten und bestenfalls sogar Geschäftsabschlüsse ein Gradmesser für die Passgenauigkeit der Werbung und liefern so wichtige Parameter für die generelle Verbesserung der Auswahlmechanismen und die Gestaltung von Werbekampagnen. Das typische Klick- und Kaufverhalten des einzelnen Nutzers ist zudem ein Merkmal, das sich in seinem Profil niederschlägt.

2.5 AKTEURE IM WERBUNGSORIENTIERTEN TRACKING-ÖKOSYSTEM

Ein Ökosystem, das den Nutzern (finanziell) kostenfreie Online-Angebote zur Verfügung stellt und sich durch Werbung finanziert, umfasst ein komplexes Geflecht von Akteuren. Den Nutzern ist davon meist nur der formale Online-Anbieter (einer Website) bekannt, beispielsweise über den Domänennamen[6] der Webadresse. Auf der entgegengesetzten Seite befinden sich die Unternehmen, die ihre Werbung möglichst erfolgreich platzieren (lassen) wollen. Die Werbenden (»Demand Side«) benötigen in zweierlei Hinsicht die Unterstützung der Online-Anbieter (»Supply Side«): beim Erfassen der Daten zur Bildung von Nutzerprofilen und beim Ausspielen der Werbung. Bei dieser Konstellation werden typischerweise Trackingdienste über integrale Bestandteile der von den Nutzern in Anspruch genommenen Online-Angebote tätig. Auch für Online-Anbieter, die nicht funktional vom Tracking profitieren – weil sie in ihren Angeboten weder kostenpflichtige Werbeplätze zur Verfügung stellen noch selbst Trackingdaten nutzen – kann es sich lohnen, Trackingdienste mit Daten zu versorgen, wenn sie von den Trackingdienstleistern dafür bezahlt werden.

Angesichts der Menge von Online-Anbietern und Werbenden sowie einer großen Vielfalt an Vermarktungsmodellen für Werbeplätze haben sich Intermediäre etabliert, denen es beide Seiten mehr oder weniger überlassen, Werbung und Nutzer möglichst Erfolg versprechend zusammenzubringen.

Auf der Seite der Werbenden sind dies typischerweise Dienstleister, die Werbende dabei unterstützen, ihre Werbung, die beworbenen Waren und Dienstleistungen und ihr Unternehmen generell bestmöglich zu charakterisieren, Adressatenkategorien festzulegen, Werbekampagnen zu planen, limitierende Preisfaktoren für Werbeauktionen (s. u.) festzulegen und Werbeplätze durch direkten Kauf oder Auktionen zu erwerben. Unterstützt werden die Planungen von Trackingdiensten, die beispielsweise statistische Daten zu Adressatenkategorien liefern und die Erfolgsdaten von Kampagnen erfassen.

Auf der Seite der Online-Anbieter sind es Dienstleister, die bei der Kategorisierung der Angebote (für kontextbasierte Werbung) und bei der »Befüllung« von Werbeplätzen über Werbemarktplätze unterstützen. Hier sind die Trackingdienste tätig, indem sie Trackingdaten erfassen und auswerten und Profildaten über den konkreten Nutzer liefern, für den ein Werbeplatz befüllt werden soll. So kann die Werbung nicht nur passend zum Seitenkontext, sondern auch zur Webhistorie des Nutzers bestimmt werden.

Logisch in der Mitte befinden sich Werbeauktionatoren, die für aktuell zu befüllende Werbeplätze – charakterisiert z. B. durch Kontext- oder Nutzerkategorien – innerhalb von Millisekunden eine Auktion durchführen.

Allerdings stellt der Zuschlag bei einer solchen Auktion oft nur den Sieg in einer Art Vorrunde dar. Oft werden Werbeplätze über mehrere Auktionatoren gleichzeitig angeboten, um die Reichweite bei den Werbenden zu erhöhen, da viele von ihnen nur mit wenigen Auktionatoren zusammenarbeiten. Anhand der Auktionsergebnisse und eigenen Wissens – z. B. über die

[6] Z. B. »online-anbieter.de«.

SOGAR MAUSBEWEGUNGEN WERDEN GETRACKT.

Auktionssieger, über weitere, simultan angezeigte Werbung oder über den Nutzer, dem die Werbung präsentiert werden soll – entscheidet typischerweise wiederum ein Dienstleister des Online-Anbieters, welche Werbung zum Zug kommt.

Die Vielzahl der an der Befüllung eines Werbeplatzes beteiligten Akteure und die kurzen verfügbaren Zeitspannen begünstigen Angriffe auf die Nutzer, indem mit der (vermeintlichen) Werbung z. B. Schadsoftware (»Malvertising«) oder rechenleistungsintensive Software (z. B. für »Kryptomining«), die ihre Ergebnisse Dritten zur Verfügung stellt, heruntergeladen wird.

Ein Sonderfall ist das individualisierte Bewerben eigener Waren und Dienstleistungen auf den Webseiten eines Unternehmens. Hier bleibt alles in der Hand des Online-Anbieters (und ggf. seiner Dienstleister).

2.6 WELCHE NUTZERAKTIONEN LÖSEN TRACKING AUS?

Beim werbungsorientierten Tracking wird typischerweise der Abruf der Webelemente aufgezeichnet, die Trackingcode enthalten. Dabei ist bedeutungslos, ob auf den entsprechenden Webseiten aus dem Tracking resultierende Werbung angezeigt wird. Handelt es sich bei diesen Abrufen um eine Reaktion auf eine zuvor angezeigte Werbung, wird auch dies mitprotokolliert.

Beim Tracking zwecks Optimierung (oder auch beim »Vorratstracking«) werden zudem Interaktionen aufgezeichnet, die eine Kommunikation mit dem Online-Anbieter auslösen, z. B. einzelne Nutzereingaben. Allerdings ist oft nicht offensichtlich, wann eine solche Kommunikation ausgelöst wird. An situationsbezogenen Wortvervollständigungsvorschlägen von Webseiten wird z. B. deutlich, dass in einem solchen Fall jedes eingegebene Zeichen direkt weitergeleitet wird. Hat der Nutzer JavaScript zugelassen und ist ein Online-Angebot entsprechend präpariert, werden sogar Mausbewegungen auf den betroffenen Bildschirmfenstern bzw. Browsertabs▸, die Abwesenheit der Maus auf diesen Fenstern/Tabs und das Schließen derselben registriert.

3. WELCHE TRACKINGDATEN LIEFERN TYPISCHE INTERNETKONTEXTE?

Unterschiedliche Internetkontexte, Anwendungsrealisierungen und Kommunikationsprotokolle▸ liefern auch unterschiedliche Daten, die im Rahmen von Tracking genutzt werden können. Die hier gewählte Klassifikation der Kontexte ist weder trennscharf noch überlappungsfrei.

3.1 IN VIELEN KONTEXTEN VERFÜGBARE BASISDATEN

Zu den Basisdaten gehört vor allem die IP-Adresse▸ des Nutzers[7], die in jedem Aufruf enthalten sein muss, um eine Antwort zustellen zu können. Fast immer werden auch Daten über die konkrete nutzerseitige Anwendung, das Betriebssystem und fundamentale Hardwareeigenschaften zur Verfügung gestellt. Die Basisdaten sind z. B. hilfreich für eine optimale Darstellung von Inhalten und eine effiziente Datenübertragung, ermöglichen aber ebenso – gemeinsam betrachtet – einen hohen Anteil eindeutig wiedererkennbarer Geräte.

Hat der Nutzer ein gegebenes Webelement▸, dem ein ETag (s. Abschnitt 5.2) zugeordnet ist, bereits in der Vergangenheit heruntergeladen (und zwischenzeitlich seinen Browsercache nicht gelöscht), wird dieses ETag beim erneuten Abruf mitgesendet.

Erfolgt der Aufruf an eine (Sub-)Domäne▸, für die bereits ein oder mehrere Cookies (s. Abschnitt 5.1) gesetzt sind, werden diese samt ihrer Werte an die (Sub-)Domäne mitgeschickt.

Loggt sich ein Nutzer bei einem Dienst ein, dann können seine Aktivitäten bei diesem Dienst mit seinen Aktivitäten bei früheren, gleichzeitigen und späteren Login-Sitzungen▸ beim selben Dienst[8] verknüpft werden. Unter bestimmten Bedingungen können sogar die Aktivitäten des Nutzers außerhalb des Dienstes (also z. B. mit anderen Websites), aber mit der IP-Adresse, die beim Login verwendet wurde, für die Dauer der Login-Sitzung diesem Nutzer zugeschrieben werden (s. dazu auch Abschnitt 4).

3.2 SOZIALE KONTEXTE

Soziale Kontexte können intensive Einblicke in Verhaltensweisen und Vorlieben, Meinungen und persönliche Werte liefern. Zu derartigen Kontexten gehören beispielsweise unwissentlich von einem Online-Dienst mitgehörte Gespräche und Audiodaten aus der Umgebung, die alltägliche Nutzung der eigenen, mit einer Smart-Home-Lösung ausgestatteten Wohnung, die oft in ihrer Tragweite unreflektierte soziale Interaktion mit Anderen in sozialen Netzen oder bei Online-Spielen und die Aufzeichnung eigener physiologischer und Verhaltensdaten im Zusammenhang mit der Alltagsgestaltung.

Unbewusste oder unwissentliche Audio-, Video- oder Positionsübermittlung

Apps lassen sich häufig Zugriffsrechte auf Mikrofon, Kamera und GPS-Empfänger▸ geben, selbst wenn dies nicht für die Funktionalität der App erforderlich ist. Es sind Fälle bekannt, dass Nutzer auf diese Art ausgespäht wurden.[9] Mikrofonzugriff beispielsweise ermöglicht dem Dienstleister umfangreiche Einblicke nicht nur in die Sprachkommunikation des Nutzers, sondern auch zu Fernseh-, Hörfunk- sowie sonstigem Video- und Audiokonsum.

Die Audiodaten, mit denen sich intelligente digitale Assistenten▸ explizit angesprochen fühlen, werden zur Auswertung an einen Server des Dienstleisters geschickt. Üblicherweise wird jede Ansprache mit einem Schlüsselwort eingeleitet. Es ist jedoch nicht ausgeschlossen, dass eine andere Phrase fälschlicherweise als Schlüsselwort interpretiert wird oder das Schlüsselwort z. B. in einer Fernsehsendung benutzt wird. In diesen Fällen kommt es zu einer unbeabsichtigten Übermittlung.

Dienstleistergestützte Smart-Home-Lösungen

Bei Smart-Home-Lösungen, die Mess- und Logdaten an den Server eines Dienstleisters schicken, ist in der Regel auch die Aufzeichnung dieser Daten durch den Dienstleister vorgesehen. Die Daten können nicht nur für den Nutzer anschaulich aufbereitet und z. B. um Vergleichswerte ergänzt werden. Der Dienstleister kann aus den Daten auch konkrete Kaufempfehlungen

[7] Die IP-Adresse wird allerdings nicht unbedingt nur von einem einzigen Nutzer verwendet, s. a. Abschnitt 4.

[8] Ggf. auch bei allen anderen Diensten eines Dienstverbundes.

[9] https://www.heise.de/newsticker/meldung/Smartphone-Spiele-belauschen-Nutzer-3928850.html.
https://www.pc-magazin.de/ratgeber/cross-device-tracking-daten-schutz-tipps-3195539.html

DURCH EINEN LOGIN WIRD PERSONENSPEZIFISCHES TRACKING MÖGLICH.

ableiten, die dem Nutzer dann beispielsweise beim Herunterladen von Verlaufsaufzeichnungen mit angezeigt werden.

Soziale Netze

Ein Zugang zu vorhandenen Daten in sozialen Netzen wie Facebook, StayFriends oder LinkedIn, das Abonnieren neuer Nachrichten z. B. bei Twitter, das Einstellen eigener Inhalte und die aktive Kommunikation mit anderen Teilnehmern eines Netzes ist meist nur möglich, wenn man sich einen Account‣ anlegt, in dem von vornherein persönliche Daten hinterlegt werden müssen. Zur Nutzung der Dienste eines sozialen Netzes ist zudem fast immer ein Login erforderlich. Dem Betreiber des sozialen Netzes wird damit die personenspezifische Aufzeichnung aller Aktivitäten im sozialen Netz (und ggf. darüber hinaus, s. Abschnitt 3.1) ermöglicht.

Bei der privaten Nutzung sozialer Netze werden häufig recht intime Inhalte eingestellt. Für sämtliche Nutzerinhalte, aber auch für das Wissen über Beziehungen jeglicher Art, das aus Aktivitäten wie Inhaltsfreigabe für bestimmte Personen oder »Liken«‣ generiert werden kann, räumt sich der Betreiber des sozialen Netzes über seine allgemeinen Geschäftsbedingungen weitgehende Nutzungsrechte ein.

Als besonders wertvoll für Werbezwecke gelten die Beziehungen zwischen den Teilnehmern eines Netzes, weil daraus typischerweise auf eine Interessenüberschneidung geschlossen werden kann. Zudem gilt Werbung, die auf eine persönlich bekannte Person referenziert (»*X* hat gerade … gekauft«) als Erfolg versprechender als unpersönliche Werbung.

Es ist bekannt, dass einige Betreiber sozialer Netze nicht nur auf die von ihren Nutzern explizit angegebenen bzw. hochgeladenen Daten zugreifen, sondern zudem Daten über Nicht-Teilnehmer des Netzes beispielsweise aus den persönlichen Telefonbüchern oder den Verbindungsaufzeichnungen ihrer Nutzer gewinnen und für diese Nicht-Teilnehmer sogenannte Schattenprofile anlegen.

Neben den für soziale Netze spezifischen Daten können auch die allgemein beim Browsen und Surfen anfallenden Daten (s. Abschnitt 3.3) gewonnen werden, da die Interaktion in der Regel über Webseiten und das Anklicken von Links‣ erfolgt.

Online-Spiele

Online-Spiele und Spiele mit Online-Funktionen können je nach Onlineanteil und Komplexität des Spiels unterschiedlich invasiv tracken: von Nutzungszeiten über Nutzungsintensität bis hin zur Aufzeichnung der einzelnen Aktionen. Während das Tracking vielfach allein der geeigneten Platzierung von Werbung für kostenpflichtige Aktionen oder andere Spiele desselben Anbieters dient, liefern Nutzungsmuster auch Hinweise auf den Tagesablauf des Spielers. Manche Fachleute meinen zudem, aus dem Spielverhalten ließen sich die aktuelle Stimmung und sogar allgemeine Eigenschaften des Spielers – wie z. B. Risikobereitschaft, Aggressivität, Teamverhalten … – ableiten.

Fitness-Tracker (und andere Online-Dienste, die mit physiologischen Daten arbeiten)

In Abhängigkeit von den jeweiligen Ausstattungsmerkmalen zeichnen Fitness-Tracker verschiedene physiologische Messdaten des Trägers (z. B. Herzfrequenz, Sauerstoffsättigung des Blutes …), seine Aktivitäten und meist auch den dynamischen Verlauf des Aufenthaltsortes auf. Zusätzlich werden von den Nutzern weitere Daten angegeben (Körpergewicht, Essprotokolle, relevante Erkrankungen …). Die Daten ermöglichen umfangreiche Rückschlüsse zum Gesundheitszustand und etwaigen Risiken, aber auch zum Tagesablauf und zu Bewegungsprofilen.

Auch aus anderen, über einen gewissen Zeitraum gewonnenen physiologischen Daten eines Nutzers (z. B. der Basaltemperatur) können Aussagen über gesundheitliche Aspekte des Nutzers abgeleitet werden.

LEITUNGSVERSCHLÜSSELTE E-MAIL-KOMMUNIKATION SCHÜTZT NICHT GEGEN AUSWERTUNG DURCH DEN ANBIETER.

3.3 KLASSISCHE INTERNETKOMMUNIKATION

Zur klassischen Internetkommunikation zählen wir den Abruf (weitgehend statischer) Webseiten sowie die bi- und multilaterale Text-, Audio- und Videokommunikation.

Browsen und Surfen

Getrackt werden vornehmlich Webseitenabrufe (mit Datum/Uhrzeit, Gerätetyp, Betriebssystem, Browserversion), aber auch Klicks auf spezielle Stellen von Webseiten bis hin zu sämtlichen Maus- und Tastaturaktionen (JavaScript vorausgesetzt) können mit genauen Zeitangaben aufgezeichnet werden.

Generell gilt: Ein Webseitenanbieter kann beliebige Abrufe von Drittanbietermaterial – z. B. Bilder, dynamische Seiteninhalte … – in seine Seiten integrieren und dabei eigenes Wissen über den Nutzer im Aufruf weitergeben. Beispiele für besondere Privatheitsunfreundlichkeit sind hier die Weitergabe von E-Mail-Adresse, Name oder Benutzername (s. dazu auch Abschnitt 5.4).

Bei Abrufen aus Webseiten heraus – per Klick auf einen Link oder bei automatischen Abrufen – ist die Webadresse der umgebenden Seite (»Referer«, s. Abschnitt 5.3) im Abruf enthalten. Ist diese Webadresse individualisiert oder sogar personalisiert (s. Abschnitt 5.4), erhält der Drittanbieter somit auch diese Informationen.[10] Dadurch gewinnen insbesondere Trackingdienstleister, deren Material in viele Seiten unterschiedlicher Online-Anbieter integriert ist, ein umfassendes, domänenübergreifendes Bild der Webnutzung des Getrackten: die aufgerufenen Seiten sowie Aktionen, die in der Seitenadresse kodiert sind – z. B. Suchanfragen, interessierende, konkrete Waren und Dienstleistungen oder sogar Authentifizierungsdaten. Daraus lassen sich auch hier Informationen zum Tagesablauf, ebenso aber z. B. zum Kaufverhalten (sofort entschlossen, vergleichend, zögernd/abwartend …) usw. ableiten. Der Webseitenanbieter hingegen erhält von den Trackingdiensten typischerweise nur die seine Website betreffenden getrackten Nutzerdaten und diese vielfach auch nur aggregiert bzw. statistisch aufbereitet.

E-Mail

E-Mails werden heutzutage fast ausschließlich direkt vom E-Mail-Anbieter des Absenders zu dem des Adressaten übertragen, wobei leitungsverschlüsselte Kommunikation der Regelfall ist. Dadurch ist ein Tracking von E-Mail durch Dritte weitgehend ausgeschlossen. Typischerweise werden E-Mails jedoch nicht Ende-zu-Ende verschlüsselt, sodass sie bei den beteiligten E-Mail-Anbietern unverschlüsselt vorliegen und dort demnach auch inhaltlich ausgewertet werden können.

Wenn E-Mail-Inhalte Webelemente abrufen oder der Nutzer auf in E-Mails enthaltene Links klickt, wird dies wie Abrufe aus einem Browser heraus behandelt. Unterstützt der benutzte E-Mail-Klient[11] Cookies (s. Abschnitt 5.1), werden diese bei entsprechenden Abrufen mitgesendet und gemäß der Antwort ggf. geändert. Sind die Webadressen der abgerufenen Webelemente bzw. die Links individualisiert oder personalisiert (s. Abschnitt 5.4), ist ein individuelles Tracking des Lesens der E-Mail möglich.

Instant Messaging

Instant Messaging wird zunehmend sowohl als SMS- als auch als E-Mail-Alternative genutzt. Im Gegensatz zum Browsen und zur E-Mail-Kommunikation kommen viele untereinander inkompatible Produkte zum Einsatz. Damit Nutzer eines Produktes miteinander in Kontakt treten können, besitzt jeder Nut-

[10] Inzwischen wird davon abgeraten, aus einer verschlüsselt abgerufenen Webseite (»HTTPS«) heraus den Referer an Drittanbieter mitzuliefern, die unverschlüsselt (»HTTP«) aufgerufen werden. Viele Browser markieren oder blockieren sogar derartige sogenannte »gemischte Inhalte«. Die Konsequenz daraus ist jedoch noch häufig, dass die Webseite selbst nur für einen unverschlüsselten Abruf bereitgestellt wird.

[11] Definition »Klient« s. Glossar.

INTERNETKONZERNE GEWINNEN DURCH TRACKING ÜBER VERSCHIEDENE DIENSTE BESONDERS DETAILLIERTE DATEN.

zer jeweils ein eindeutiges Kennzeichen, anhand dessen ihm sowohl versendete als auch empfangene Nachrichten zugeordnet werden können.

Bzgl. der Möglichkeiten und der Haltung von Anbietern zum Tracking von Nutzern existiert ebenfalls ein breites Spektrum: Manche Instant-Messaging-Klienten verschlüsseln Nutzerinhalte Ende-zu-Ende, wobei alle zum Entschlüsseln benötigten Schlüssel bei den Klienten verbleiben. Andere verschlüsseln zwar Ende-zu-Ende, der Messaging-Anbieter besitzt aber Kopien der kritischen Schlüssel und könnte damit Einsicht in die Nutzerinhalte nehmen. Bei unverschlüsselten oder nur leitungsverschlüsselten Diensten kann der Anbieter alle Inhalte auswerten.

Üblicherweise meldet sich ein Nutzer bei einem Instant-Messaging-Dienst an, wenn er kommunikationsbereit ist. Teilweise werden auch detailliertere Bereitschaftszustände unterstützt. Versand und Empfang aller Nachrichten sowie der Status der Kommunikationsbereitschaft können nutzerindividuell vom Anbieter getrackt werden. Daraus können Rückschlüsse auf den Tagesablauf und auf Beziehungen zu anderen Personen gezogen werden.

Bei manchen Instant-Messaging-Diensten sind neben dem Nutzerkennzeichen weitere identifizierende Daten, z. B. der Name, abgelegt. Dies ermöglicht das Suchen nach Personen, deren Nutzerkennzeichen man noch nicht kennt, aber auch die Zuordnung von Trackingdaten zu konkreten Personen.

Video- und Voice-over-IP

Soweit für derartige Zwecke nicht ein »klassischer« Dienst eines Telekommunikations- und Internet-Dienstanbieters▸, sondern ein sogenannter Over-the-Top-Dienst▸ (OTT-Dienst) genutzt wird, behalten sich die Online-Anbieter häufig ein sehr weitgehendes Recht zur Auswertung der Kommunikationsbeziehungen[12] und -inhalte – auch für Werbezwecke – vor. Da die Geltung des Fernmeldegeheimnisses nach dem Telekommunikationsgesetz[13] für OTT-Dienste nach wie vor nicht eindeutig geregelt ist, ist davon auszugehen, dass teilweise tatsächlich inhaltliches Tracking stattfindet. Beispielsweise ist denkbar, dass Kommunikationsinhalte nach Stichworten durchsucht werden, die Hinweise auf werbungsrelevante Interessen der Kommunikationspartner liefern.

3.4 ZENTRALE INTERNETDIENSTLEISTER

Zentrale Internetdienstleister interagieren mit einer Vielzahl von Nutzern oder sind an einer Vielzahl von Online-Diensten (mittelbar) beteiligt, wodurch sie besonders vielfältige Trackingdaten sammeln können.

Internetkonzerne und Online-Anbieter mit großen Nutzerzahlen

Konzerne mit einem breiten Portfolio an Internet-bezogenen Dienstleistungen (z. B. Inhalts-, Kommunikations-, Marktplatz-, Tracking-, Werbedienste) können durch Tracking von Nutzern über verschiedene Dienste hinweg – Webseitenabrufe, Suchanfragen, eigene und fremde Aktivitäten in sozialen Netzen … – besonders detaillierte Nutzerprofile generieren. Daten, die aus verschiedenen Online-Diensten gewonnen wurden – z. B. aus zeitlich nebeneinander genutzten Diensten mit und ohne Login – lassen sich zueinander in Beziehung setzen, wodurch auch (allein betrachtet) weitgehend anonyme Daten individuellen Nutzern zugeschrieben werden können.

---

[12] Viele Online-Anbieter gehen damit weit über die allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten hinaus, die sogar für staatliche Zwecke vom Europäischen Gerichtshof als unzulässig eingestuft wurde (Urteil vom 21.12.2016 - C-203/15, C-698/15),

[13] Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 10 Absatz 12 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618) geändert worden ist.

WENN ONLINE-SHOPS AN WERBEDIENSTLEISTER ADRESSEN WEITERGEBEN, KÖNNEN DIESE MIT NUTZERPROFILEN ABGEGLICHEN WERDEN.

Zentrale Online-Anbieter mit großen Nutzerzahlen und häufiger Nutzung wie Suchmaschinen- oder E-Mail-Anbieter können bereits aus einzelnen Diensten einen erheblichen Detailgrad bei ihren Nutzerprofilen erreichen, der sich sowohl aus den ihnen zugänglichen Inhalts- und Adressdaten als auch aus dem spezifischen Nutzerverhalten (z. B. bevorzugt ausgewählte Suchergebnisse oder vorrangig gelesene E-Mails) speist.

»Internet-Beschleuniger«▸, die von verschiedenen Internetkonzernen angeboten werden, leiten in der Regel zumindest einen Teil der Abrufe von Webelementen über eigene Server und können diese so tracken.

Kunden von Werbedienstleistungen liefern den Anbietern weitere Daten, die derartige Zuordnungen ermöglichen, wenn sie E-Mail- oder Postadressen eigener Kunden oder Interessenten weitergeben. Diese Daten können dann beispielsweise mit den Nutzerprofilen sozialer Netze abgeglichen werden.

Synergieeffekte entstehen beispielsweise, wenn ein Internetkonzern Daten über direkte und mittelbare Nutzer gewinnt, indem er organisatorische Unterstützung für Veranstaltungen anbietet: Durch ein Terminplanungs- oder Anmeldeportal lassen sich z. B. spezifische Interessen und Beziehungen zwischen Personen ermitteln. Diese Informationen können zur Ergänzung von Nutzer- und Schattenprofilen genutzt werden.

Content Delivery Networks (CDNs)

Content Delivery Networks, die im Auftrag von Online-Anbietern Webelemente ausliefern, erhalten mit den entsprechenden Abrufen durch Nutzergeräte alle typischen Daten, die bei einem Webabruf mitgesendet werden, und können auch Cookies auf den Nutzergeräten verwenden. Content Delivery Networks, mit denen viele Online-Anbieter zusammenarbeiten, können so einen übergreifenden Einblick in das Verhalten der entsprechenden Nutzer gewinnen. Manche CDNs sind eng mit Trackingdiensten verbunden, denen so wertvolle Trackingdaten zur Verfügung stehen.

Internetanbieter▸

Im Gegensatz zu den Online-Anbietern ermöglichen die Internetanbieter den Zugang zum Internet und die Internetkommunikation an sich. Da nach wie vor ein Großteil dieser Kommunikation unverschlüsselt stattfindet und sich bereits aus den stets unverschlüsselt gesendeten Ziel-IP-Adressen wertvolle Daten ableiten lassen, nutzen auch Anschlussanbieter die Kommunikation ihrer Kunden, um Trackingprofile für diese anzulegen[14] und beispielsweise auf ihren Webseiten dementsprechend ausgewählte Werbung zu platzieren.

Auch Trackingdienstleister sind daran interessiert, direkt die gesamten Daten an Nutzeranschlüssen analysieren zu können,[15] da ihre Reichweite bezüglich eines konkreten Nutzers damit nicht auf die Online-Dienste beschränkt wäre, die mit ihnen zusammenarbeiten.

Die unverschlüsselten Daten können von allen Routern im Internet, die sie weiterleiten, ausgewertet werden. Ob und in welchem Umfang von weiteren Betreibern Daten zu Werbezwecken gewonnen werden, ist allerdings unbekannt.

Cloudnutzung

In einer Cloud unverschlüsselt gespeicherte oder genutzte Daten können vom Cloudbetreiber prinzipiell ausgewertet werden, um beispielsweise Eigenschaften und Vorlieben eines Nutzers zu ermitteln. Der Verlauf der Cloudnutzung, Art, Zeitpunkt und Ort des Zugriffs und die Menge der Nutzer konkreter Datenobjekte liefern weiteres Material für die Profilbildung.

---

[14] Vgl. S.J.Res.34 – A joint resolution providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Federal Communications Commission relating to «Protecting the Privacy of Customers of Broadband and Other Telecommunications Services«.115th Congress (2017-2018), die als Gesetz 115-22 am 03.04.2017 in Kraft trat und verschiedene Privatheitsrechte von Nutzern gegenüber Internetanbietern annullierte.

[15] http://news.bbc.co.uk/2/hi/technology/7325451.stm.

3.5 SOFTWARE UND APP STORES

Software jeglicher Art wird mehr und mehr mit Funktionen ausgestattet, um automatisch Nutzungs-, Leistungs- und Fehlerdaten an den Hersteller zu schicken und dort oder im App Store ihren Aktualitätsstatus abzufragen, selbst wenn sie anscheinend offline benutzt wird.

App Stores

App Stores als zentrale Marktplätze für Anwendungssoftware für ganz bestimmte Gerätefamilien können anhand des Such- und Kauf- bzw. Downloadverhaltens der Nutzer sehr genaue Informationen über deren Interessen und Vorlieben, deren individuellen Gerätepark sowie über die Art der Nutzung jedes einzelnen Gerätes (z. B. überwiegend beruflich oder eher privat) gewinnen. Die sichere Nutzerzuordnung ist dabei durch die notwendige Authentifizierung selbst für das Herunterladen kostenloser Software durchgängig gegeben. Da installierte Software regelmäßig den App Store kontaktiert, um festzustellen ob ein Softwareupdate verfügbar ist, können auch der Onlinestatus des Gerätes und der Installationsstatus der Software getrackt werden. Besitzübergänge von Geräten sind ebenfalls feststellbar, da zumindest kostenpflichtige Software meist an eindeutige Geräteidentifikatoren gebunden wird.

Anbieter von Browsern und Browser-Add-ons

Da beim Browserstart automatisch umfangreiche Aktualitätsabfragen stattfinden, haben auch hier die Anbieter einen guten Überblick über den Installationsstatus. Der Mix der Browser-Add-ons ist vielfach sehr individuell, wodurch die vom selben Nutzer verwendeten Geräte einem einzigen Nutzerprofil zugeordnet werden können. Rückschlüsse auf den Lebensrhythmus des Nutzers lassen sich ziehen, wenn man davon ausgeht, dass auf vielen Geräten der Standardbrowser automatisch beim Einschalten des Gerätes gestartet wird.

Betriebssysteme und (sonstige) Anwendungen

Je nach Detailgrad der an den Hersteller gesendeten Daten, der Anzahl der Anwendungen desselben Herstellers auf dem fraglichen Gerät und der Nutzungsintensität lassen sich beispielsweise Rückschlüsse ziehen, ob es sich um ein beruflich oder privat genutztes Gerät handelt und wie geübt der Nutzer im Umgang mit dem Gerät, dem Betriebssystem und den Anwendungen ist.

	Beziehungen zwischen Personen	Interessen/Werte/ Vorlieben	Gewohnheiten (Tagesablauf, An-/ Abwesenheit …)
Audio-/Video-/ Positionsübermittlung	durch Inhaltsauswertung	X	
Smart Home (dienstleistergestützt)	ggf. durch Inhaltsauswertung		
Soziale Netze	X	X	X
Online-Spiele	X		X
Fitness-Tracker (u. Ä.)	X (bei der Nutzung integrierter Social-Media-Funktionen); durch Inhalteverknüpfung	in Bezug auf körperliche Betätigung	X
Browsen/Surfen	durch Inhaltsauswertung	X	
E-Mail	X	durch Inhaltsauswertung	X
Instant Messaging	X	durch Inhaltsauswertung	X
Video-/Voice-over-IP	X	durch Inhaltsauswertung	
Konzerne/ Großanbieter		X (besonders vielfältige/detaillier-te Möglichkeiten!)	X (besonders vielfältige/detaillier-te Möglichkeiten!)
CDNs		X	X
Internetanbieter (bei unver-schlüsselter Kommunikation)	durch Inhaltsauswertung	durch Inhaltsauswertung	X (auch bei verschlüsselter Kommunikation!)
unverschlüsselte Cloudnutzung		durch Inhaltsauswertung	X
App Stores		Nutzertyp (z. B. spielorientiert, nachrichtenorientiert)	
Browser/-Add-on-Anbieter			X (wenn nicht »always-on«)
Anbieter von Betriebssystemen und sonstigen Anwendungen			X

REGISTRIERUNG ERMÖGLICHT KONKRETEN PERSONENBEZUG.

Private Inhalte Text/Bild	Positions-/Ortsdaten (zusätzlich: stets grob anhand IP-Adresse)	Name, Adresse, E-Mail-Adresse, evtl. Kreditkartennr.	Logindaten für andere Online-Angebote	Physiologische Daten
X	X bei Positionsübermittlung			
ggf. durch Inhaltsauswertung	bei Anwesenheit	X		
X	X (wenn »geteilt«)	wenn Registrierung erforderlich	X (wenn Anbieter Login-Provider ist)	durch Inhaltsauswertung
		wenn Registrierung erforderlich		
X (bei der Nutzung integrierter Social-Media-Funktionen)	X	wenn Registrierung erforderlich		X
	X (wenn Positionsübermittlung freigegeben)			durch Inhaltsauswertung
durch Inhaltsauswertung		wenn Registrierung erforderlich	durch Inhaltsauswertung	durch Inhaltsauswertung
durch Inhaltsauswertung		wenn Registrierung erforderlich	durch Inhaltsauswertung	durch Inhaltsauswertung
durch Inhaltsauswertung		wenn Registrierung erforderlich		durch Inhaltsauswertung
durch Inhaltsauswertung	bei Kopplung der Internetnutzung und an den Festnetz-/ Mobilfunkvertrag	X	durch Inhaltsauswertung	durch Inhaltsauswertung
durch Inhaltsauswertung		wenn Registrierung erforderlich		durch Inhaltsauswertung
		X		
	X (wenn Positionsübermittlung freigegeben)	wenn Registrierung erforderlich		

4. STUFEN DER WIEDERERKENNBARKEIT

Je nachdem, wie lange und bei welchen unterschiedlichen Aktivitäten ein Nutzer wiedererkennbar ist, bestimmen sich die Menge der getrackten Daten, die sich mit dem Nutzer in Verbindung bringen lässt, und die Menge der Daten, die daraus wiederum abgeleitet werden kann. So steigt der Wert der Daten in der Regel überproportional zur Menge der aufgezeichneten Trackingdaten. Nach einer gewissen Beobachtungsdauer lassen sich beispielsweise relativ genaue Aussagen über den Tagesablauf der Nutzer machen.

Aus Sicht der wirtschaftlichen Akteure beim Tracking wird daher umfassende Wiedererkennbarkeit angestrebt. Nutzer hingegen, die nicht zum Beobachtungs-, Aus- und Verwertungsobjekt werden möchten oder die sich schlichtweg unwohl fühlen, wenn ihnen unbekannte Dritte offenbar sehr persönliches Wissen über sie besitzen, haben ein Interesse daran, genau dies zu vermeiden, ohne dabei jedoch auf die Nutzung bestimmter Dienste oder Inhalte im Internet verzichten zu müssen.

Wiedererkennbarkeit bezieht sich im Folgenden stets auf die Wiedererkennung durch ein und dieselbe Webdomäne‣. Ohne das Zutun weiterer Domänen, beispielsweise einer abrufenden Domäne[16], sollten moderne Internetanwendungen keine Wiedererkennung ermöglichen, bei der aktiv auf Daten anderer Domänen zugegriffen wird. Z. B. Gedankenlosigkeit bei der Datenweitergabe an Trackingdienste und Programmierfehler in Browsern haben aber auch dies in der Vergangenheit verschiedentlich zugelassen. Bekannt ist zudem, dass Online-Anbieter Trackingdienstleistern eigene Cookie-Daten explizit zur Verfügung stellen (»Cookie-Matching«) und so die Wiedererkennung z. B. bei Werbeauktionen (s. Abschnitt 2.5) ermöglichen.

Keine Wiedererkennung erforderlich

In vielen Fällen ist es nicht erforderlich, einen Internetnutzer überhaupt wiederzuerkennen, um einen bestimmten Dienst für ihn zu erbringen oder ihm die Nutzung bestimmter Daten zu ermöglichen. Z. B. das Herunterladen von öffentlich, kostenlos und beliebig häufig zugänglichen Dokumenten benötigt weder eine Authentisierung des Nutzers noch eine Aufzeichnung der Downloadhistorie. Jeder dieser Downloads kann funktional alleinstehend und unabhängig von allen anderen erfolgen.

Wiedererkennung während einer expliziten Domänensitzung

Eine explizite Domänensitzung beginnt mit dem Abruf einer Webseite der Domäne oder dem Start einer App, die mit der Domäne kommuniziert. Sie endet, wenn der Nutzer das entsprechende Browserfenster, den Browsertab oder die App schließt oder sich bei der Website abmeldet. Eine derartige Wiedererkennbarkeit kann erforderlich sein, wenn dem Nutzer erst nach einer Authentisierung bestimmte Funktionen oder Daten zur Verfügung stehen oder wenn Ereignisse der Sitzung temporär aufgezeichnet werden müssen, z. B. der Inhalt eines digitalen Warenkorbes oder das Durchlaufen bestimmter Lerninhalte.

Diese Wiedererkennung kann vollständig über Cookies (s. Abschnitt 5.1) umgesetzt werden, die nicht über die Domänensitzung hinaus gültig sein müssen. Eine häufig eingesetzte Alternative, die ohne Cookies funktioniert, ist die Ergänzung von Webseitenadressen und Links durch individuelle Session IDs‣ (s. Abschnitt 5.4).

Wiedererkennung während der Benutzung einer lokalen Anwendungsinstanz‣ (Session‣)

Diese Form der Wiedererkennbarkeit besteht individuell für bestimmte Anwendungen (z. B. Browser, E-Mail-Reader oder Apps) auf einem IT-Gerät und nur bis diese Anwendungen jeweils beendet werden. Bei Browsern wird in diesem Zusammenhang auch oft von einer Session gesprochen. Es gibt keinen prominenten Anwendungsfall, der genau diese Form der Wiedererkennung benötigt, aber alle modernen Browser unterstützen sie auf einfache Art und Weise, indem die lokal von Webelementen gespeicherten Daten am Ende der Browsersession gelöscht werden können. Deshalb wählen diese Form der Wiedererkennbarkeit sowohl Online-Angebote als auch Nutzer als – allerdings weitergehende – Alternative zur Wiedererkennbarkeit während einer Domänensitzung (s. Abschnitt 4). Die generelle Wahl dieser Form der Wiedererkennbarkeit durch den Nutzer sollte deshalb nicht dadurch verhindert werden, dass – wie heute üblich – speziell Antitracking-Mechanismen auf permanent, über Browsersessions hinweg (in Cookies) gespeicherten Daten basieren.

Diese Wiedererkennung kann komplett über sogenannte Session Cookies (s. Abschnitt 5.1) realisiert werden. Authentisiert sich beispielsweise ein Nutzer in einer Browsersession (mit

[16] Wird beispielsweise durch das Anzeigen der E-Mail eines Online-Händlers beim Nutzer ein Abruf bei einem Trackingdienstleister initiiert, kann der Online-Händler dabei Daten mitschicken lassen, die auch eine domänenübergreifende Wiedererkennung von Einzelwesen oder gar konkreten Personen ermöglichen.

AUCH BEIM PRIVATEN BROWSEN
VERRINGERN COOKIES DIE PRIVATHEIT.

Benutzername/Passwort oder einem anderen Mittel) an einem öffentlich zugänglichen Gerät in einem Hotel, muss er sicher sein können, dass in einer zukünftigen Session (vermutlich eines anderen Nutzers) diese Authentisierung nicht mehr gültig ist. Die trackende Seite kann von sich aus Session Cookies setzen, der Nutzer kann eine Anwendungseinstellung wählen, bei der *alle* Cookies bei Beendigung der Anwendungsinstanz verworfen, also wie Session Cookies behandelt werden. Bei öffentlich zugänglichen Geräten sollte eine entsprechende Anwendungseinstellung fixiert sein.

Exkurs: Was ist eine Browserinstanz (Browsersession) und was passiert beim »privaten« Browsen?
Eine Browserinstanz darf nicht mit einem einzelnen Browserfenster oder Browsertab verwechselt werden – in der Regel gehören alle Fenster und Tabs, die zwischen Start und Beendigung der Anwendung geöffnet werden, zur selben Instanz. Das Schließen von Fenstern oder Tabs führt nicht dazu, dass die darin gesetzten Session Cookies gelöscht werden, sie können in anderen Fenstern und Tabs derselben Session weiterbenutzt werden. Nur sehr wenige Browser unterstützen überhaupt den Betrieb voneinander unabhängiger Instanzen.[17] Nur in diesem Fall werden sämtliche Einstellungen und Aufzeichnungen der Instanzen getrennt gehalten.

Während des sogenannten privaten oder inkognito Browsens werden Cookies in den entsprechenden Fenstern unabhängig von denen in den allgemeinen Browserfenstern, ansonsten aber gemäß ihren Eigenschaften behandelt. In einem solchen Fenster gesetzte Cookies stehen also auch den anderen derartigen Fenstern zur Verfügung. Existiert kein privates/inkognito Fenster mehr, werden alle in diesem Modus gesetzten Cookies gelöscht. Die gleichzeitige Nutzung mehrerer Seiten kann also auch beim privaten Browsen die Privatheit verringern.

Wiedererkennung einer bestimmten Anwendung auf demselben Gerät
Online-Anbieter können die erneute Benutzung einer bestimmten lokalen Anwendung auf demselben Gerät (sogar über verschiedene Anwendungsversionen hinweg) immer dann sicher erkennen, wenn die Anwendung ihnen ermöglicht, dauerhaft individuelle Daten auf dem Gerät zu speichern, die bei der Kommunikation mitgesendet werden, z. B. permanente Cookies (s. Abschnitt 5.1). Ansonsten ist (mit den im folgenden Unterabschnitt beschriebenen Einschränkungen) vielfach die Wiedererkennung bereits anhand allgemeiner Anwendungs- und Gerätemerkmale und der IP-Adresse möglich.

Wiedererkennung von Geräten
Die Wiedererkennung von Geräten ist ein mit verschiedenen Methoden leicht zu erreichendes Trackingziel.

Jeder Bereitsteller von Webelementen (z. B. auch ein Content Delivery Network, CDN, s. Abschnitt 3.4) kann Downloads seiner Webelemente anhand der stets im Abruf enthaltenen IP-Adresse des abrufenden Gerätes einem Geräteprofil zuordnen. Da einige Kommunikationsformen auf eine während der gesamten Kommunikation gleichbleibende IP-Adresse angewiesen sind, wird diese meist nur selten geändert.[18] Wegen der seltenen Änderung ist es durchaus wahrscheinlich, dass selbst eine erst nach längerer Zeit erneut auftauchende IP-Adresse nach wie vor demselben Internetanschluss, evtl. sogar demselben Gerät exklusiv zugeordnet ist, sofern der Nutzer seine IP-Adresse nicht (z. B. durch Nutzung des Tor-Netzwerkes) verschleiert. Für diese einfachste, aber auch am wenigsten detaillierte Wiedererkennung von Geräten anhand der IP-

[17] Lt. der aktuellen Browser-Abgleichstabelle des Bundesamtes für Sicherheit in der Informationstechnik (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Browser-Abgleich_Mindeststandard_Sichere_Web-Browser.pdf?__blob=publicationFile&v=3) besitzt Firefox diese Funktionalität, mit Google Chrome lässt sie sich eingeschränkt realisieren.

[18] Die Deutsche Telekom beispielsweise vergibt an einem Anschluss mit dynamischer IP-Adresse erst nach maximal 180 Tagen eine neue Adresse, wenn der Kundenrouter ununterbrochen eingeschaltet war.

OFT REICHT DIE WIEDERERKENNUNG EINES GERÄTES, UM AUF EINE BESTIMMTE PERSON SCHLIESSEN ZU KÖNNEN.

Adresse werden keine zusätzlichen Daten für die Trackingunterstützung auf den Nutzergeräten gespeichert. Andererseits handelt es sich bei der IP-Adresse um ein personenbeziehbares Datum, dessen Speicherung, z. B. bei einem Trackingdienstleister, besonderen Anforderungen unterliegt.

Bei Privat- und kleinen Businessanschlüssen »teilen« sich in der Regel mindestens alle Geräte, die einen gemeinsamen Kundenrouter benutzen, dieselbe IP-Adresse.[19] Sie ist also nicht unbedingt exklusiv einem Nutzer zugeordnet. Neben IP-Adressdaten enthält jeder Webabruf standardmäßig die verwendete Browserversion, das Betriebssystem und die bevorzugte Sprache. Diese allein ermöglichen ebenfalls keine eindeutige Geräteidentifikation, in Kombination mit der IP-Adresse (und ggf. anderen Geräteeigenschaften) kann jedoch häufig ein individuelles, wiedererkennbares Geräteprofil erzeugt werden. Damit sind dann die (üblicherweise alleinigen) Nutzer des Gerätes ebenfalls wiedererkennbar.

Umgekehrt können mobile Geräte, die alternativ eine IP-Adresse eines Mobilfunkanbieters und einen bestimmten Privat- bzw. Businessanschluss benutzen, über vielfach vorhandene und für Tracking zugreifbare eindeutige Identifikatoren (wie IMEI▸, Android-ID, Werbe-ID …) oder ihre gleichbleibenden Geräteeigenschaften auch bei Mobilfunknutzung diesem Anschluss und seinen Nutzern zugeordnet werden, insbesondere wenn bei beiden Nutzungsformen häufig dieselben Internetaktivitäten (Abrufen bestimmter Webseiten usw.) stattfinden.

Wiedererkennung eines »digitalen Schattens«▸ an einem bestimmten Gerät

Bei dem in diesem Dokument vorrangig betrachteten wirtschaftlich motivierten Tracking für Online-Werbezwecke benötigt keiner der beteiligten Akteure einen Bezug zu den realen Personen, die getrackt werden. Es reichen Profile, die die verhaltensbestimmenden Eigenschaften, Meinungen, Vorlieben und das Verhalten einer realen Person ausreichend umfassend und detailliert beschreiben, um sie mit möglichst großen Erfolg versprechender Werbung versorgen zu können.

Für diesen Zweck müssen die Profile keine unmittelbaren Identifikatoren wie Name oder Adresse enthalten.[20] Wir unterscheiden daher zwischen der Wiedererkennung sozusagen gesichts- und namenloser »digitaler Schatten« mit einem bestimmten Satz werbungsrelevanter Eigenschaften und der Wiedererkennung konkreter realer Personen mittels eindeutig beschreibender Identifikatoren (s. dazu den späteren Unterabschnitt). Auch ein detailliertes Profil ohne eindeutige Identifikatoren kann allerdings so individuell sein, dass es nur zu einer realen Person passt – das Herausfinden dieser Person erfordert jedoch in der Regel mehr als nur einen Blick in ein geeignetes Verzeichnis.

Da viele IT-Geräte wie PCs, Smartphones und Tablets in der Regel nur von einer Person benutzt werden, ist die Annahme berechtigt, beim Wiedererkennen eines Gerätes (s. vorheriger Unterabschnitt) immer wieder denselben »digitalen Schatten« zu tracken und mit Werbung ansprechen zu können, die auf diesen abgestimmt ist. Ist an einem Gerät ein untypischer Nutzungsmix, womöglich mit bestimmten zeitlichen Regelmäßigkeiten, beobachtbar – z. B. das Streamen von Romantikfilmen einerseits und von Filmen mit gewalttätigen Inhalten andererseits –, dann kann auf eine Nutzung durch mehrere Personen geschlossen werden[21]. Bei nicht eindeutig personaspezifischen Tätigkeiten, z. B. dem Konsum aktueller Nachrichtensendungen, kann dann nicht auf einen bestimmten »digitalen Schatten« gefolgert werden.

[19] Diese Darstellung bezieht sich auf das nach wie überwiegend eingesetzte IP-Protokoll Version 4, kurz IPv4. Die Situation kann sich zukünftig beim Einsatz von IPv6 ändern.

[20] E-Mail-Adressen (soweit verfügbar) werden allerdings eventuell verwendet, um Werbe-E-Mails zu versenden. IP-Adressen, Benutzerkennungen und E-Mail-Adressen können zudem die Wiedererkennung erheblich erleichtern.

[21] Solche Schlussfolgerungen sind nicht zwangsläufig korrekt, aber empirische Beobachtungen rechtfertigen eine derartige Verallgemeinerung.

INDIVIDUALISIERTE WERBE-E-MAILS ERMÖGLICHEN OFT GERÄTEÜBERGREIFENDE WIEDERERKENNUNG.

Ruft ein Nutzer immer wieder dieselbe Webseite auf – z. B. die Einstiegsseite einer bestimmten Websuche oder eines anderen Webdienstes – ist er anhand des ETags (s. Abschnitt 5.2) der Seite wiedererkennbar, sofern dieses individualisiert ist.

Bei ausreichend detailliertem Tracking der Nutzeraktionen (s. Abschnitt 2.6) kann die Bediengeschwindigkeit und -charakteristik der Tastatur, aber auch von Maus oder Spielsteuerungsgerät als individueller elektronischer »Fingerabdruck« genutzt werden.

Wiedererkennung eines »digitalen Schattens« über verschiedene Geräte hinweg

Aus der Sicht von Werbetreibenden und Trackingdienstleistern ist es besonders erstrebenswert, Nutzer über alle benutzten IT-Geräte hinweg tracken und mit Werbung versorgen zu können. Einerseits ist so eine noch präzisere Personazuordnung und -gestaltung möglich, andererseits kann die Werbung auf den einzelnen Geräten aufeinander abgestimmt werden.

Ein Mittel sind beispielsweise automatische individualisierte Trackingabrufe beim Öffnen von Werbe-E-Mails: Wird die E-Mail auf dem Smartphone überflogen und später auf einem PC erneut geöffnet, um sich über die enthaltenen Links die beworbenen Produkte anzuschauen, können beide Geräte dauerhaft mit demselben Nutzerprofil verknüpft werden. Jede spätere Nutzung eines der Geräte kann – mit der üblichen Unsicherheit – dem Nutzer zugeschrieben werden.

Synchronisiert der Nutzer Browsereinstellungen und -zustände zwischen Geräten, werden dabei Lesezeichen und für einige Browser auch (permanente) Cookies synchronisiert, was ebenfalls geräteübergreifendes Tracking ermöglichen kann (s. dazu die Abschnitte 5.1 bzw. 5.4).

Werden – z. B. beruflich und privat – ausreichend ähnliche Geräte genutzt, ist auch eine Wiedererkennung über den elektronischen Fingerabdruck (s. vorheriger Unterabschnitt) möglich.

Wiedererkennung konkreter Personen

Die Wiedererkennbarkeit konkreter Personen – über z. B. Name, E-Mail-Adresse, Mobilfunknummer …, zunehmend aber auch über biometriebasierte Authentifizierungsmittel wie Fingerabdrücke oder Gesichtserkennung – ist eine Möglichkeit, um unabhängig voneinander generierte, zu derselben Person gehörende Nutzerprofile zusammenzuführen.

Fehlende, zu einem Profil passende Daten lassen sich beispielsweise aus Registrierungsdaten für Online-Dienste, Verzeichnissen (Sprach-/Videotelefonie, Zertifikate, öffentliche Kryptografieschlüssel …) und Inhaltsdaten (E-Mails, Instant Messaging …) ermitteln.

Zu dieser Art der Wiedererkennung kann auch die IP-Adresse beitragen: Die zeitnahe oder sogar zeitlich verschränkte Nutzung verschiedener Online-Dienste mit derselben IP-Adresse lässt – vor allem, wenn die Zielgruppen der Dienste in wesentlichen Profildaten wie Geschlecht, Altersgruppe oder Interessenkategorien übereinstimmen – vielfach die berechtigte Vermutung zu, dass es sich dabei um dieselbe Person handelt.

5. TRACKINGMITTEL UND -METHODEN

Alle hier beschriebenen Mittel und Methoden werden – unterschiedlich intensiv – zum Tracking von Nutzern (bzw. deren Geräten) genutzt. Da ständig nach neuen Trackingmöglichkeiten gesucht wird, insbesondere um Gegenmaßnahmen der Nutzer, Add-on-Entwickler und Browserhersteller umgehen zu können, liefern die erwähnten Mittel und Methoden kein vollständiges und abschließendes Bild.

Mit Ausnahme der Zählpixel dienen diese Mittel und Methoden auch anderen Zwecken, weshalb nicht generell von Tracking ausgegangen werden kann, wenn Webseiten sie benutzen. Dies erschwert ein gezieltes Vorgehen der Nutzer gegen das Tracking.

Zunächst werden Parameter der Webkommunikation aufgeführt, die nutzer- (bzw. geräte-)individuelle Daten transportieren können, dann die Hilfsmittel, an die diese Parameter gebunden sind oder die die Werte der Parameter beeinflussen können. Abschließend werden Möglichkeiten genannt, individuelle Daten mittels der lokalen Hard- und Softwareumgebung des Nutzers zu gewinnen.

5.1 COOKIES

Cookies‣ sind prinzipiell beliebige Daten, die mit der Antwort auf einen Webabruf auf dem Gerät des Nutzers gespeichert werden. Standard-Cookies werden beim Abruf jedes weiteren Webinhalts derselben, häufig auch jeder nebengeordneten Subdomäne‣ automatisch an den Anbieter zurückgeschickt, für andere Cookie-Typen kann dies mittels JavaScript (s. Abschnitt 5.7) veranlasst werden. Cookies können mit jeder Antwort aktualisiert werden. Sie sind ein generelles Mittel, um Zustandsinformation auf dem Nutzergerät zu speichern, z. B. ob der Nutzer eingeloggt ist. Da mit ihnen das Herunterladen von Webelementen verfolgt werden kann, sind sie allerdings auch das am verbreitetsten genutzte Trackingmittel.

Cookies können nicht domänenübergreifend genutzt werden. Es wird zwischen sogenannten Erstanbieter‣- und Drittanbieter-Cookies unterschieden. Für Tracking verwendete Cookies sind typischerweise Drittanbieter-Cookies und »gehören« dem Trackingdienst, da das Tracking meist durch Dienste erfolgt, zu denen ein Nutzer nicht intendiert Kontakt aufnimmt. Bei derartigen Aufrufen werden *sämtliche* Standard-Cookies des jeweiligen Trackingdienstes automatisch mitgeschickt und durch die Antworten ggf. aktualisiert. Ist JavaScript eingeschaltet, können auch die Werte anderer Cookie-Typen in beide Richtungen übermittelt werden. Tracking-Cookies wirken Website-übergreifend für alle Websites, die Elemente des entsprechenden Trackingdienstes einbinden, also aus dessen Domäne herunterladen. Ein Beispiel: Der Nutzer hat sich bei einem Online-Händler, der mit Trackingdienst *T* zusammenarbeitet, ein bestimmtes Produkt angesehen. Der Trackingdienst hat die Information über das Produkt und den Händler durch einen Trackingaufruf aus der beim Nutzer angezeigten Webseite heraus erhalten und ein entsprechendes Cookie mit einem nutzerindividuellen Wert gesetzt. Schaut sich der Nutzer nun ein ähnliches Produkt bei einem anderen Online-Händler an, der ebenfalls mit Dienst *T* zusammenarbeitet, kann der Trackingdienst beide Aktivitäten demselben Nutzerprofil zuordnen.

Bei der lokalen Ausführung von JavaScript-Code (s. Abschnitt 5.7) kann dieser Cookies seiner Domäne lokal direkt setzen und ändern und dies auch dem Anbieter der bereitstellenden Domäne mitteilen.

Permanente Cookies
Trackingdienste setzen für ihre Cookies typischerweise eine unbegrenzte oder sehr lange Gültigkeitsdauer. Sie existieren also über das Ende der Anwendungsinstanz hinaus.

Permanente Cookies werden aber beispielsweise auch benutzt, um den individuellen Wiedereinstieg in einen Online-Lehrgang zu ermöglichen.

Session Cookies
Vom setzenden Anbieter als solche gekennzeichnete Session Cookies werden beim Beenden der lokalen Anwendungsinstanz automatisch gelöscht. Eine Wiedererkennung über diese Cookie-Art ist also nur innerhalb der laufenden Anwendungsinstanz möglich.

Der Nutzer kann z. B. bei Browsern zudem typischerweise einstellen, dass auch die permanenten Cookies wie Session Cookies behandelt und beim Beenden der Anwendungsinstanz gelöscht werden.

Kritik im Zusammenhang mit Cookies
Die Nutzer wissen oft nicht, wozu ein bestimmtes Cookie eingesetzt wird und ob die betroffene Website noch wie gewünscht

ANHAND VON ETAGS KÖNNEN AUCH EXPLIZIT GELÖSCHTE COOKIES REKONSTRUIERT WERDEN.

funktioniert, wenn sie (einzelne oder generell alle) Cookies verhindern.

Ein sehr großer Teil der während einer komplexeren Nutzeraktivität[22] erfassten und der daraus produzierten Daten ist nur relevant, bis der Vorgang abgeschlossen ist. Werden derartige Daten in Cookies gespeichert, dann nutzen nur wenige Websites die Möglichkeit, die Daten anschließend sofort explizit zu invalidieren[23]. Sie werden meist lediglich als »bei Beendigung des Browsers/der App zur Löschung freigegeben« markiert, schlimmstenfalls sogar mit einem deutlich in der Zukunft liegenden expliziten Verfallsdatum versehen. Dies ist nicht im Sinne der Speicherbegrenzung und kann auch einen mangelnden Schutz gegen unbefugte oder unrechtmäßige Nutzung darstellen: Gelingt Dritten der Zugriff auf derartige Daten, ist im ungünstigen Fall der Missbrauch der Identität des Nutzers (zumindest bzgl. dieser Website) möglich.

Ähnliches gilt für Daten, die der Wiedererkennung während einer Domänensitzung dienen: Erkennt der genutzte Online-Dienst das Ende der Domänensitzung (z. B. durch einen Abmeldevorgang), sollte er entsprechende Cookies explizit invalidieren. Generell sollten für diesen Zweck nur Session Cookies benutzt werden, damit die Cookies auch bei Nichterkennung eines früheren Endes der Domänensitzung spätestens beim Beenden der Anwendungsinstanz verfallen.

5.2 ETAGS

Ein ETag ist eine beliebige Zeichenkette, die einem (Tracking-) Webelement (z. B. einem Zählpixel, s. Abschnitt 5.5) von seinem Bereitsteller zugeordnet wird. Solange sich das Element dann im Speicher eines Browsers befindet, wird bei jedem weiteren Abruf des – vielleicht inzwischen veränderten – Elementes das ETag mitgeschickt. Ist das Element noch aktuell, wird nur diese Tatsache quittiert und das Element nicht erneut übertragen, das ETag jedoch eventuell geändert. Ursprünglich zur Vermeidung des mehrfachen Downloads identischer Inhalte gedacht, werden ETags mit einem nutzerindividuellen Wert[24] zum Tracking benutzt. ETags werden im Trackingkontext auch verwendet, um vom Nutzer bei Beendigung der Anwendungsinstanz gelöschte Cookies wiederherstellen zu können. Wird dabei der lokale Zwischenspeicher für Web-Inhalte nicht gelöscht, kann der Bereitsteller beim nächsten Abruf des Tracking-Webelementes die Beziehung zu den bei ihm spiegelbildlich gespeicherten Cookies herstellen und diese beim Nutzer erneut setzen.

Die »Last-Modified«[25]-Daten eines Webelementes können in gleicher Weise verwendet werden.

Kritik im Zusammenhang mit ETags

ETags sind vor dem Nutzer verborgen und können von ihm nicht individuell gelöscht werden. Auch ein Löschen durch den setzenden Bereitsteller ist nicht möglich.

ETags beim Nutzer können nur gelöscht werden, indem dort der gesamte lokale Zwischenspeicher für Online-Inhalte (»Cache«) gelöscht wird.

5.3 REFERER

Beim Abruf eines Webelementes über einen in einer Webseite enthaltenen Link wird die vollständige Webadresse der Quellwebseite – des Referers – mitgeschickt. Damit kann beispielsweise festgestellt werden, in welchem Kontext eine allgemeine

[22] Beispielsweise die Auswahl eines Videos zwecks Streamings, die entsprechende Bezahlung und das eigentliche Streaming.

[23] Websites können Cookies nicht explizit löschen, ihnen aber ein sofortiges oder in der Vergangenheit liegendes Verfallsdatum zuordnen, das den Browser veranlassen sollte, das Cookie nicht mehr zu verwenden.

[24] Bzw. einem individuellen Wert für das Nutzergerät.

[25] Auf Deutsch: »letztmalig geändert«.

Funktion oder Grafik zum Einsatz kommen soll, und dies ggf. durch den Server blockiert werden. Trackingdiensten liefert der Referer die genaue Seitenadresse. Ist diese zudem individualisiert oder gar personalisiert (s. Abschnitt 5.4), können die entsprechenden Daten vom Trackingdienst direkt genutzt werden.

Kritik im Zusammenhang mit dem Referer

Die Referer-Übermittlung erfolgt vor dem Nutzer verborgen und die Beziehung zu individualisierten Webseitenadressen ist nicht offensichtlich. Eine datenarme Konfiguration ist nicht mittels der Standard-Benutzerschnittstelle des Browsers möglich.

5.4 INDIVIDUALISIERUNG▸ UND PERSONALISIERUNG▸ VON WEBSEITENADRESSEN[26] UND LINKS

Ein Webserver▸ kann eine gegenüber dem Abruf veränderte Webseitenadresse zurücksenden.

Individualisierung durch eine Session ID

Bei dieser Methode wird die allgemeine Webseitenadresse durch ein individuelles Kennzeichen für eine Domänensitzung, eine **Session ID**[27]▸, ergänzt. In der Regel werden auch alle in der Webseite enthaltenen Links entsprechend geändert. Aktualisiert nun der Nutzer die Seite, klickt er einen Link an oder es wird automatisch ein Webelement abgerufen, können alle diese Abrufe über die Session ID einander zugeordnet werden.

Während manche Websites diese Methode alternativ oder ergänzend zu Cookies einsetzen, um aus inhaltlichen Gründen einen Sitzungszustand oder -verlauf aufzuzeichnen und zuzuordnen, kann sie ebenso zum Tracking verwendet werden. Speichert der Nutzer eine derartige Webseitenadresse als Lesezeichen oder eine Webseite mit entsprechend individualisierten Links, wird die Session ID bei jeder Nutzung des Lesezeichens oder dem Anklicken eines Links auf der gespeicherten Seite erneut mitgesendet. Bei der Weitergabe entsprechender Links an Dritte und deren Nutzung der Links kann über diese Daten eine Verbindung zum Profil des ursprünglichen Nutzers hergestellt werden. So ist auch über einen langen Zeitraum eine Wiedererkennung von Nutzern bzw. eine Erkennung von Beziehungen zwischen Nutzern möglich.

Personalisierung

Eine verschärfte Form der Individualisierung von Webseitenadressen und von Links auf Webseiten bzw. in E-Mails ist die Parametrisierung mit Identifikatoren der betroffenen Person: die Personalisierung[28]. Nach wie vor sind hier z. B. **Namen, Benutzerkennungen, Passwörter und E-Mail-Adressen** im Klartext und oft auch in Kombination zu beobachten.

Kritik im Zusammenhang mit individualisierten und personalisierten Webseitenadressen und Links

Individualisierte Webseitenadressen und Links können weder vom Anbieter beim Nutzer invalidiert noch vom Nutzer mit einfachen Mitteln »ent-individualisiert« werden. Der Nutzer kann nicht überprüfen, ob oder wann der Anbieter die Verknüpfung derartiger Daten mit etwaigen erfassten und beim Anbieter gespeicherten, den Nutzer identifizierenden Daten löscht. Viele Nutzer bemerken individualisierte, oft sogar personalisierte Adressen von Webelementen nicht oder sind sich der Tragweite der übermittelten Daten nicht bewusst.

Besonders kritisch zu bewerten sind personalisierte Links zu (Tracking-)Drittanbietern und personalisierte Webseitenadressen. Diese Daten stehen damit auch dem Drittanbieter (direkt

[26] Auch als »URL Rewriting« bezeichnet, wobei diese allgemeinere Bezeichnung allerdings nicht individualisierende Änderungen ebenfalls umfasst, z. B. das nutzerunabhängige Hinzufügen von Datum und Uhrzeit.

[27] Beispiel: »http://www.beispieldomaene.de/index.html?**jsessionid=abcde12345**«.

[28] Beispiel: »beispieldomaene.de/start.html?**user=mueller**«.

ZÄHLPIXEL BESITZEN KEINEN DIREKTEN WERT FÜR DEN NUTZER.

aus der Adresse des von ihm bereitgestellten Webelementes oder über den Referer, s. Abschnitt 5.3) zur Verfügung, können mit seinen Trackingdaten bzgl. des Nutzers verknüpft werden und ermöglichen evtl. eine domänenübergreifende Zusammenführung verschiedener Profile derselben konkreten Person. Derartige langfristig gültige Identifikatoren ermöglichen zusammen mit anderem Wissen über den Nutzer auch die Zuschreibung getrackter zurückliegender und zukünftiger Aktivitäten des abstrakten Nutzers zu einer realen Person.

Weitere Dritte, denen so prinzipiell die Wiedererkennung konkreter Personen ermöglicht wird, sind z. B. Content-Delivery-Dienstleister (s. Abschnitt 3.4), die für den Online-Anbieter tätig werden, E-Mail-Dienstleister, aber auch – bei unverschlüsselter Übertragung von Webaufrufen – Internetanbieter.

Selbst wenn derartige Daten nicht im Klartext, sondern nur als Hash-Werte‣ übertragen werden, ist die Zuordnung zum konkreten Nutzer für jeden Dritten möglich, der Zugriff auf die Webseitenadresse bzw. den Link erhält, den jeweiligen Aufbau (er)kennt, die nutzerspezifischen Daten bereits aus einem anderen Kontext besitzt (z. B. aus einer beobachteten Klartextindividualisierung) und der somit die Hashwerte nach den bekannten Verfahren ebenfalls berechnen kann. Wem Kombinationen aus Namen, Benutzernamen und E-Mail-Adressen bekannt werden, der kann auch alle Aufrufe einander zuordnen, die nur eines oder einige der Daten enthalten.

Ein Online-Anbieter, bei dem die Eingabe der Logindaten eines Nutzers *X* zum Aufruf einer immer gleichen Webseitenadresse führt, die – gleichgültig ob im Klartext, als Hash-Werte oder anderweitig codiert – Benutzerkennung und Passwort enthält[29], schafft damit zudem gute Voraussetzungen für einen Identitätsmissbrauch. Da viele Nutzer nach wie vor dasselbe Passwort für mehrere Dienste benutzen, kann unsensibles Vorgehen bereits eines Online-Anbieters – die Klartextangabe des Passwortes in einer Webseitenadresse bzw. einem Link – vielfachen Missbrauch der Identität der betroffenen Nutzer ermöglichen.

5.5 ZÄHLPIXEL‣

Zählpixel sind winzige, meist völlig durchsichtige und farblose »Bilder«, die vom Betrachter einer Webseite in der Regel nicht bemerkt werden. Sie werden durch die Webseite automatisch von fremden (Tracking-)Domänen hinzugeladen und dienen dazu, diesen Domänen den Abruf der Webseite zu signalisieren. So könnte nur ein Abrufzähler realisiert werden. Mit dem Abruf erhält die Fremddomäne allerdings für Trackingzwecke geeignete Daten: die üblichen Daten, die bei einem Webaufruf mitgeschickt werden (z. B. Cookies und Referer, s. a. Abschnitt 3.1) sowie etwaige bezüglich des Zählpixels beim Nutzer bereits vorhandene Daten wie ein ETag (S. Abschnitt 5.2). Zusätzlich kann die abrufende Webseite Informationen über den Nutzer an den Dienst schicken, z. B. als Parameter des Abrufes. Manchmal werden auch Informationen über die abrufende Webseite oder über den Nutzer direkt im Namen des Zählpixels codiert.

Kritik im Zusammenhang mit Zählpixeln
Zählpixel bieten keinen inhaltlichen Wert für den Nutzer. Der Abruf von Zählpixeln erfolgt vor dem Nutzer verborgen und kann nur mit hohem Aufwand verhindert werden. Es gibt keine Möglichkeit, generell nur das Herunterladen von Zählpixeln zu blockieren.

5.6 WEBSEITENGESTALTUNG

Viele Webseiten verwenden Gestaltungshilfsmittel[30], die von Drittanbietern – häufig Internetkonzernen – zur Verfügung gestellt werden. Beim Herunterladen der Hilfsmittel werden

[29] Beispiel: »http://beispieldomaene.de/logon?**name=x&passw=xpass**«.

[30] Cascading Style Sheets (CSS. Gestaltungsvorlagen), Fonts und grafische Elemente.

MITTELS JAVASCRIPT KÖNNEN COOKIES LOKAL GESETZT UND GEÄNDERT WERDEN.

Cookies (s. Abschnitt 5.1) sowie ETags und ähnliche Daten (s. Abschnitt 5.2) ausgetauscht und der Referer (s. Abschnitt 5.3) übermittelt.

Kritik im Zusammenhang mit Gestaltungshilfsmitteln von Dritten

Der Abruf von Dateien für die Webseitengestaltung erfolgt vor dem Nutzer verborgen. Ein bewusster Verzicht auf die Gestaltungshilfsmittel durch den Nutzer führt in der Regel zu so erheblichen Einschränkungen der Usability‣ und des Nutzungserlebnisses der Webseite, dass dies selbst nur von sehr wenigen der Nutzer umgesetzt wird, die Tracking ablehnend gegenüberstehen. Viele Webseiten könnten jedoch so gestaltet werden, dass sie auch ohne die Hilfsmittel akzeptabel nutzbar sind.

5.7 JAVASCRIPT

Die bisher beschriebenen Trackingmittel und -methoden benötigen keinen Einsatz von JavaScript. Mit JavaScript können jedoch weitere Eigenschaften des benutzten Gerätes (Hard- und Software) und des Browsers (s. Abschnitt 5.9) abgefragt und in Trackingabrufen weitergereicht werden. Bereits durch die Kombination weniger dieser Eigenschaften lassen sich die meisten Geräte eindeutig identifizieren.[31] Nutzer, die ihre Browserkonfiguration über mehrere Geräte hinweg vereinheitlichen, z. B. zwischen dem Arbeitsplatz- und dem heimischen PC, schaffen so – zumindest wenn sie, z. B. gerade zum Schutz ihrer Privatheit, Browsereinstellungen verändert und viele Add-ons installiert haben – geräteübergreifende Identifikationsmöglichkeiten.

Ebenso können – wie bereits in Abschnitt 5.1 angesprochen – mittels JavaScript Cookies der jeweiligen Domäne gesetzt und geändert werden, z. B. abhängig von Aktionen des Nutzers.

Da auch die statischen, nicht auf JavaScript angewiesenen Inhalte von Webseiten in JavaScript-abhängigen Code »verpackt« werden können, kann eine Seite so gestaltet werden, dass sie unbrauchbar ist, wenn man die Ausführung von JavaScript unterbindet.

JavaScript ermöglicht zudem das Tracking sämtlicher Nutzeraktionen auf einer Webseite (s. Abschnitt 5.10).

Kritik im Zusammenhang mit JavaScript

JavaScript ist für die Funktionalität vieler Webseiten essenziell[32] und der Abruf und die Ausführung von JavaScript-Code für Tracking können nicht gezielt verhindert werden.

5.8 HTML5-CANVAS-ELEMENT

Die heutzutage von allen aktuellen Browsern unterstützte HTML5-Spezifikation bietet die Möglichkeit, mittels JavaScript dynamisch eine Grafik zu erzeugen. So können beispielsweise Visualisierungen unter Berücksichtigung von Nutzereingaben lokal auf dem Nutzergerät erzeugt werden.

Da die Darstellung auf einem Nutzergerät in der Regel wegen der vielfältigen eingesetzten Hard- und Software sehr individuell ausfällt und bestimmte Darstellungsergebnisse abgefragt werden können, lässt sich die Wiedererkennung eines Gerätes über die Nutzung eines Canvas-Elementes realisieren (»Canvas Fingerprinting«).

[31] Wie einzigartig die eigene Gerätekonfiguration innerhalb einer nicht repräsentativen Menge von Freiwilligen ist, kann man beispielsweise unter https://panopticlick.eff.org oder https://amiunique.org testen.

[32] Bevor die Ausführung von JavaScript-Code zugelassen wird, kann oft nicht einmal festgestellt werden, dass bestimmte Funktionen ohne JavaScript nicht oder nur eingeschränkt zur Verfügung stehen,

ELEKTRONISCHE FINGERABDRÜCKE KÖNNEN SENSIBLE NUTZEREIGENSCHAFTEN OFFENBAREN.

Kritik im Zusammenhang mit Canvas Fingerprinting
Canvas Fingerprinting erfolgt vor dem Nutzer verborgen, das Website-spezifische Verhindern ist aufwendig.[33]

5.9 HARD- UND SOFTWARE-EIGENSCHAFTEN DES BENUTZTEN GERÄTES

Wie bereits in Abschnitt 3.1 angesprochen, sind einem Online-Anbieter vielfältige Daten über Hardwareeigenschaften des Nutzergerätes – z. B. Bildschirmparameter oder die Ausstattung mit bestimmten Ein- oder Ausgabegeräten – und auf dem Gerät vorhandene Software – z. B. Browsertyp, -version und -einstellungen, installierte Add-ons und deren Einstellungen, Spracheinstellungen – zugänglich. In Summe bieten diese Daten häufig die Möglichkeit, das Gerät eindeutig wiederzuerkennen. Ein Teil dieser Daten wird automatisch mit jedem Webaufruf mitgesendet. Weitere Daten können z. B. Webseiten lokal abfragen und dem Online-Anbieter mitteilen, wozu dann in der Regel die Verwendung von JavaScript erforderlich ist.

Kritik im Zusammenhang mit der Abfrage und Übermittlung von Geräteeigenschaften
Die Abfrage und Übermittlung von Geräteeigenschaften erfolgt vor dem Nutzer verborgen, eine vollständige Liste dieser Eigenschaften ist nicht leicht einsehbar. Die Übermittlung kann nur mit erheblichem Aufwand verhindert werden.

5.10 ELEKTRONISCHE FINGERABDRÜCKE VON NUTZERN

JavaScript ermöglicht das Tracking sämtlicher Nutzeraktionen auf einer Webseite, von Mausbewegungen bis zu »nicht abgeschickten« Eingaben, und das alles mit genauen Zeitangaben. Funktionen, die man im Zusammenhang mit Auto-Vervollständigen, vorhersagenden Eingabevorschlägen oder automatisch erscheinenden Erläuterungen als komfortabel empfindet, ermöglichen einerseits ein sehr detailreiches, intimes Tracking und andererseits die Erstellung von Nutzerprofilen, die einen Nutzer geräteunabhängig wiedererkennbar machen können. Das Verhalten von Nutzern kann so feingranular aufgezeichnet und ausgewertet werden, dass daraus individuelle Bedienecharakteristika, z. B. bei Maus und Tastatur, abgeleitet werden können. Auch für die Aufzeichnung und Auswertung von Umgebungsgeräuschen wurden bereits verblüffende Ergebnisse berichtet.[34]

Kritik im Zusammenhang mit elektronischen Fingerabdrücken
Die Erfassung elektronischer Fingerabdrücke erfolgt vor dem Nutzer verborgen. Als besonders kritisch zu bewerten ist, dass elektronische Fingerabdrücke sensible Eigenschaften eines Nutzers, z. B. eine Rechtschreibstörung oder eine Parkinson-Erkrankung, offenbaren können.

[33] Allerdings werden Canvas-Elemente bei breit genutzten Online Angeboten noch so selten für die Darstellung von für die Nutzer relevanten Inhalten eingesetzt, dass ein generelles Verhindern dieser Funktionalität durch den Nutzer in der Regel nicht zu Einschränkungen von Usability und Nutzungserlebnis führt. Bemerkbare funktionale Einschränkungen können bei lokal gezeichneten, dynamischen grafischen Darstellungen auftreten.

[34] S. Gould: »A Novel Approach to User Authentication Through Machine Learning of Keyboard Acoustic Emanations«; https://pdfs.semanticscholar.org/9b2d/4e57387bf2a6d515b095d0af1ac3502c2b8a.pdf.

6. TRACKING IM LICHT DER EU-DATENSCHUTZ-GRUNDVERORDNUNG

Je nach Art, Umfang und Detailreichtum können Trackingdaten, insbesondere wenn sie aus Inhaltsdaten der Nutzer gewonnen werden, selbst dann personenbezogen oder in hohem Maße personenbeziehbar sein, wenn eine Wiedererkennung konkreter Personen (s. Abschnitt 4) weder erforderlich noch beabsichtigt ist. Die Regeln des Datenschutzes gelten daher in vielen Fällen und sind spätestens seit dem Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO)[35] im Mai 2018 auch dann von Online-Anbietern und den von ihnen genutzten Trackingdienstleistern einzuhalten, wenn diese außerhalb der EU angesiedelt sind. Damit gelten generell die Grundsätze der Datenminimierung (Art, Umfang und Detailreichtum), Speicherbegrenzung (Aufbewahrungsdauer) und Zweckbindung.

Ob die gewählte Art der Erhebung und Verarbeitung von Daten für Tracking und individualisierte Werbung erforderlich ist – eine privatheitsfreundlichere Vorgehensweise der Online-Anbieter dies also nicht leisten kann –, dürfte in vielen Fällen strittig sein. Es kann auch nicht davon ausgegangen werden, dass die berechtigten Interessen der Tracking-Ökosysteme die der Internetnutzer an Privatheit in der Regel überwiegen. Die Datenschutzkonferenz[36] bezweifelt zudem, dass bei umfassendem, domänenübergreifendem Tracking die Nachvollziehbarkeit der Verarbeitung durch den Nutzer gewährleistet werden kann. Deshalb werden viele Online-Anbieter und Trackingdienstleister ihr Vorgehen voraussichtlich weiterhin auf der Einwilligung der Nutzer abstützen. Die Nutzer müssen dazu allerdings zukünftig nachweisbar und weitaus detailreicher über den Zweck informiert werden.

Die DSGVO legt bezüglich der Grundprinzipien »Datenschutz durch Technikgestaltung« (»Privacy-by-Design«) und »datenschutzfreundliche Voreinstellungen« (»Privacy-by-Default«) für die Erhebung und Weiterverarbeitung von Trackingdaten durch vielfältige Akteure (s. Abschnitt 3) vielleicht eine ausreichende, durch detailliertere Regulierung und die Rechtsprechung gestaltbare Basis. Schwieriger wird es bei den Hilfsmitteln, die beispielsweise von Browsern zur Verfügung gestellt werden. Cookies z. B. werden für unterschiedliche Zwecke benutzt, die nicht alle datenschutzrelevant sind. Eine generelle Voreinstellung, die Cookies im Browser nicht zulässt, greift daher zu weit und wird kaum den angestrebten Effekt – Datenminimierung – unterstützen. Vielmehr ist zu erwarten, dass die Nutzer beim ersten durch fehlende Cookies auftretenden Problem diese undifferenzierte Einstellung dauerhaft ändern.

Gesundheitsdaten unterliegen einem besonderen Schutz und umfangreichen Verarbeitungsverboten durch die DSGVO. Selbst wenn – was vermutlich der Regelfall ist – ein Nutzer der Verarbeitung physiologischer Daten durch Fitness-Tracker und ähnliche Online-Dienste zugestimmt hat, lassen sich aus den erfassten Daten häufig deutlich weiter reichende Schlüsse ziehen als den Nutzern bewusst ist. Ob eine auf diese weiter reichenden Schlüsse abzielende Verarbeitung und insbesondere die Nutzung der so gewonnenen Erkenntnisse im konkreten Fall tatsächlich zulässig sind, dürfte in starkem Maße von der konkreten Gestaltung der Zustimmung und der – ggf. auch gerichtlichen – Beurteilung der Freiwilligkeit der Zustimmung abhängen.

---

[35] 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).

[36] Datenschutzkonferenz: »Kurzpapier Nr. 3 – Verarbeitung personenbezogener Daten für Werbung«, Stand 29.06.2017, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Kurzpapier_Werbung.pdf?__blob=publicationFile&v=2.

7. INTERNETTRACKING – CHANCEN UND RISIKEN FÜR DIE NUTZER

Aus Sicht der Online-Werbewirtschaft ist Individualisierte Werbung eine folgerichtige Entwicklung:

- Mit gegebenen Werbeetats sollen möglichst große Umsätze erzielt werden,
- dazu müssen bestenfalls nur die Personen angesprochen werden, die durch die Werbung am ehesten zur Umsatzgenerierung motiviert werden können,
- zu den diesbezüglich vorteilhaften Eigenschaften, Vorlieben, Verhaltensweisen … derartiger Personen gibt es bereits empirisches Material[37],
- das Verhalten von Internetnutzern kann leicht und meist ohne merkliche Leistungseinbuße der genutzten Dienste aufgezeichnet werden und
- Werbung, die anhand des aufgezeichneten bzw. erwarteten Verhaltens individuell ausgewählt wurde, kann leicht in Online-Angeboten, z. B. auf Webseiten oder als Pop-up, platziert werden.

Aus gesamtgesellschaftlicher Perspektive und individueller Nutzersicht kann Internettracking allerdings auch eine Reihe unerwünschter oder zumindest beunruhigender Folgen haben.

Passgenauere Werbung
Wurde ein Nutzer aus Sicht eines Werbeökosystems korrekt eingeschätzt, dann interessiert ihn die angezeigte Werbung vermutlich deutlich mehr als andere Werbung, die alternativ möglich gewesen wäre. In diesem Fall empfindet er die Werbung in der Regel als weniger störend als andere Werbung, eventuell aber (gleichzeitig) auch als irritierend bis bedrohlich.

Bestenfalls besteht tatsächlich ein Bedarf und die Werbung liefert dem Nutzer relevante Informationen, die er sonst mit höherem Aufwand hätte ermitteln müssen. Passgenaue Werbung kann aber (z. B. wegen ihrer Kosten und der Eigeninteressen der über die Ausspielung der Werbung Entscheidenden) auch dazu führen, dass der Nutzer nur den Eindruck umfassender Information hat und sich für ein Werbeangebot entscheidet, obwohl dies für ihn sachlich oder wirtschaftlich nicht optimal ist.

Einfluss auf den Preis von Waren oder Dienstleistungen
Durch domänenübergreifendes Tracking – und sofern ihm ein Trackingdienst dies mitteilt – kann ein Anbieter von Waren oder Dienstleistungen erfahren, ob ein Nutzer sich auch bei anderen Anbietern für ein bestimmtes Angebot interessiert hat und seinen Preis ggf. entsprechend anpassen.

Ebenso kann ein Anbieter von Waren/Dienstleistungen zögernde Kunden durch das Signalisieren von Knappheit (»nur noch … verfügbar«) zum Abschluss drängen.

Die auf der Basis von Tracking angenommene Kaufkraft eines Nutzers und seine Vorliebe für bestimmte Marken können auch genutzt werden, ihm Angebote mit einem vergleichsweise hohen Preis zu machen, wenn davon ausgegangen werden kann, dass er diesen akzeptieren wird.

Besonders kritisch ist, dass dem Nutzer bei einer derartigen Vorgehensweise die Möglichkeit eines neutralen Preisvergleichs genommen wird. Eine nutzerindividuelle Preisgestaltung erschwert zudem die private wie öffentliche Diskussion über Preisangemessenheit, weil Nutzer die Preise nicht kennen, die anderen Personen genannt wurden.

Ergonomischere Online-Dienste, besser verständliche Inhalte bei Webseiten …
Wird Tracking genutzt, um Schwachstellen beim Webseiten- bzw. Online-Spiele-Design zu beseitigen und die Inhalte besser zu vermitteln, führt dies zu einem besseren zukünftigen Nutzungserlebnis.

Verschlechterung des Nutzungserlebnisses bei Online-Diensten / Erosion von Datenvolumen
Umfangreiche Trackingaktivitäten führen insbesondere bei leistungsschwachen Nutzergeräten oder geringen verfügbaren Übertragungsraten zu einer Verschlechterung des Nutzungserlebnisses bezüglich der genutzten Online-Inhalte.

Tracking und Aktivitäten zum Einblenden individualisierter Werbung können ein Vielfaches des für die genutzten Online-Inhalte erforderlichen Datenvolumens verbrauchen und damit die Kosten für manche Nutzungsformen (z. B. Nicht-EU-Roaming) deutlich erhöhen.

[37] Z. B. aus den Bereichen Zeitschriften- und TV-Werbung.

EINE AUSSCHLIESSLICHE PRÄSENTATION (VERMEINTLICH) ERWÜNSCHTER INFORMATIONEN BEGÜNSTIGT EINSEITIGKEIT.

Angemessene Behandlung – oder Verstetigung von Diskriminierung

Sorgfältig und neutral durchgeführtes Tracking kann wertvolle Hinweise auf günstige Eigenschaften eines Nutzers liefern, z. B. für eine Kreditentscheidung.

Z. B. die Studie von Datta et al.[38] zeigt allerdings auch, dass mittels Tracking (wie auch auf andere Art und Weise) gewonnene Daten, die – ihrem Kontext entrissen – als Basis für zu einfache, unreflektierte Schlussfolgerungen benutzt werden, zu einer diskriminierenden Ungleichbehandlung von Nutzerkategorien (hier einer Nicht-Präsentation hoch dotierter Stellenanzeigen bei weiblichen Nutzern) führen können.

Da große Teile der Datenerfassung und -analyse inzwischen ausschließlich automatisiert ablaufen, werden derartige Folgen kaum noch offenbar und Menschen bewusst, zumal bereits bei der Implementierung nicht der thematische Einzelfall, sondern eine riesige Klasse vermeintlich statistisch gleichbehandelbarer Fälle betrachtet wird.

Begünstigung von Filterblasen‣, Echokammern‣, gesellschaftlicher Zersplitterung und Meinungsbeeinflussung

Werden den Nutzern Web-Inhalte (auf der Basis von Tracking) zunehmend individualisiert bereitgestellt, beeinträchtigt dies die einheitliche Wahrnehmung von Sachverhalten und damit die gesellschaftliche Auseinandersetzung darüber. Über die individuelle Priorisierung von Inhalten durch Dritte kann nicht nur im Konsumbereich (Werbung), sondern auch in gesellschaftlichen Fragen die Meinungsbildung beeinflusst werden. Werden beispielsweise bestimmte Inhalte kritischen Gruppen nur sehr nachrangig präsentiert, dafür empfänglichen und unkritischen Gruppen jedoch mit hoher Priorität, kann damit der Reaktionszeitpunkt der kritischen Gruppen verzögert werden.

Die vornehmliche Versorgung der Nutzer mit Web-Inhalten, die ihre Vorlieben und Meinungen bestärken, kann zudem den Eindruck erwecken, die jeweiligen Vorlieben und Meinungen seien generell vorherrschend und so die eigene kritische Auseinandersetzung damit behindern.

Beeinträchtigung der informationellen Selbstbestimmung

Es kann davon ausgegangen werden, dass die meisten Formen des Internettrackings eine Beeinträchtigung der informationelle Selbstbestimmung der getrackten Personen darstellen: Vermutlich ist in den meisten Fällen weder eine wohlinformierte Zustimmung zur gesamten tatsächlichen Nutzung der Trackingdaten erfolgt noch liegen die Daten ausschließlich in derart anonymisierter Form vor, dass eine Re-Identifizierung einzelner getrackter Personen oder kleiner, sensibler Personengruppen dauerhaft und sicher ausgeschlossen ist.

In vielen Fällen gibt es darüber hinaus Hindernisse technischer, informationeller oder praktikabler Art, die verhindern, dass die getrackten Personen ihr Recht auf informationelle Selbstbestimmung ausüben können. Die Trackingmechanismen laufen vor dem Nutzer verborgen ab und nur in Einzelfällen existiert ein leichter Zugang der Nutzer zu den Trackingmitteln und -methoden, d. h. Werte können eingesehen und gelöscht werden und die Nutzung von Methoden kann eingeschränkt werden.

Identifizierbarkeit bei Offenlegung oder Weitergabe mangelhaft anonymisierter Daten[39]

Der steigende Wert auch »anonymisierter« und aggregierter Trackingdaten begünstigt die freiwillige Weitergabe solcher Daten durch Trackingdienste und Online-Anbieter gegen Bezahlung.

[38] A. Datta, M. C. Tschantz, A. Datta: »Automated Experiments on Ad Privacy Settings«, Proceedings on Privacy Enhancing Technologies, Band 2015, Heft 1, S. 92 – 112, ISSN 2299-0984, https://www.degruyter.com/view/j/popets.2015.1.issue-1/popets-2015-0007/popets-2015-0007.xml.

[39] »A Face Is Exposed for AOL Searcher No. 4417749«, New York Times, 10.08.2006, http://www.nytimes.com/learning/teachers/featured_articles/20060810thursday.html.

BEI TRACKINGDATENSÄTZEN SIND AUSSAGEN ÜBER DIE QUALITÄT EINER ANONYMISIERUNG OFT SCHWIERIG.

Die Langzeitanonymisierung personenbeziehbarer Daten unter Wahrung möglichst vieler Auswertungsdimensionen ist schwierig, komplex und in der Regel nicht automatisiert durchführbar. Bei Trackingdaten kommt erschwerend hinzu, dass oft nicht ausreichend viele Daten über die Grundgesamtheit vorhanden sind, um eine Aussage über die Anonymisierungsqualität zu ermöglichen.[40] Zudem ist es schwierig, eine hohe Anonymisierungsqualität gegenüber Datennutzern zu erzielen, die unbekanntes Zusatzwissen über die Personen besitzen, auf die sich die Daten beziehen oder auf die sich die Daten nicht beziehen.[41]

Ein bei der Weitergabe von Trackingdaten oft übersehenes Problem sind beispielsweise personalisierte Webseitenadressen, die personenbezogene Daten enthalten, welche entweder direkt angegeben oder auf einfache Art rückführbar sind.[42]

Identifizierbarkeit für staatliche Stellen

Selbst unter der Annahme aktuellen rechtsstaatlichen Handelns aller Beteiligten kann eine unerwünschte Identifizierung in der Zukunft nicht ausgeschlossen werden, wenn heutige Daten aufbewahrt und irgendwann unter veränderten rechtlichen Rahmenbedingungen ausgewertet werden. Da gegenüber staatlichen Stellen bei gegebenem Anlass in der Regel eine sehr umfassende Auskunftspflicht besteht, ist auch die Wahrscheinlichkeit hoch, dass zumindest aus verschiedenen Quellen zusammengeführte Daten vielfach die Identifizierung konkreter Nutzer ermöglichen.

---

[40] Ignoriert beispielsweise eine mangelhafte Anonymisierung die Tatsache, dass die Rot-Grün-Sehschwäche und die Bluterkrankheit fast nur bei männlichen Personen auftreten, und versucht, durch Löschung der Geschlechtsangabe eine höheres Anonymitätsqualität zu erreichen, ist nach wie vor die Annahme statistisch berechtigt, dass die Menschen mit erfasster Rot-Grün-Sehschwäche oder Bluterkrankheit männlich sind.

[41] Kennt jemand die individuellen Mietpreise in einem bestimmten Gebiet, dann kann dieses Gebiet auch sehr groß gewählt sein: Sofern die Zahl der Haushalte mit Sozialhilfebezug in diesem Gebiet nicht wesentlich kleiner ist als die der Wohnungen mit für Sozialhilfeempfänger zulässigen Mieten, kann ziemlich genau bestimmt werden, wo Sozialhilfeempfänger wohnen. Hat jemand Einblick in das Wählerverzeichnis und somit Kenntnis über die Adressen der Nichtwähler, kann evtl. anhand der Adresse auch in einem Haus mit vielen Bewohnern ein Wähler einer bestimmten Partei identifiziert werden.

[42] Vgl. https://www.ndr.de/nachrichten/netzwelt/Nackt-im-Netz-Millionen-Nutzer-ausgespaeht,nacktimnetz100.html.

8. HANDLUNGSEMPFEHLUNGEN

Die Informationspflichten der EU-Datenschutz-Grundverordnung eng auslegen.

Sind die Anbieter gezwungen, für jedes Cookie konkrete Nutzungsangaben zu machen, dann können trackingskeptische Nutzer rein dem werbungsbezogenen Tracking dienende Cookies gezielt ablehnen, ohne funktionale Einbußen befürchten zu müssen.

Recht auf Nicht-Tracking etablieren.

Aus der Sicht der Datensouveränität der Nutzer ist es vorteilhaft, wenn diese in einfacher Form und für die Trackenden verbindlich – generell oder für bestimmte Webdomänen – festlegen können, dass sie nicht getrackt werden wollen. Zumindest bei werblichen Webseiten, Online-Shops und Seiten der öffentlichen Hand sollten mit einem Trackingverbot keine funktionalen Einschränkungen verbunden sein dürfen.

Recht auf Nicht-Verknüpfung von Profilen etablieren.

Nutzer haben vielleicht noch eine korrekte Vorstellung, welches Wissen aus dem Tracking ihres Verhaltens hinsichtlich einzelner Websites bzw. Online-Angebote gewonnen werden kann – websiteübergreifend fällt das schon sehr viel schwerer. Deshalb sollte es einfach und verbindlich möglich sein, Erstanbieterübergreifende Profilbildung zu verhindern und zu untersagen.

Sinnvolles, mehrstufiges System zum Konfigurieren der Tracking-/Verknüpfungserlaubnisse vorschreiben.

Ein sinnvolles System muss sich an den Zielen der Nutzer und nicht an den eingesetzten technischen Mitteln orientieren und den Nutzern verständlich präsentiert werden. Es darf nicht selbst auf Mitteln (z. B. Cookies) basieren, die privatheitssensible Nutzer nur sparsam bzw. nur temporär einsetzen wollen.

Die Pflicht zu Privacy-by-Design und Privacy-by-Default konkretisieren.

Ohne Löschungs- bzw. Anonymisierungs-/Pseudonymisierungsfristen und Kriterien für eine wirksame Anonymisierung/Pseudonymisierung bleiben zu viele Ermessens- und Interpretationsspielräume, als dass die Erhebung und Speicherung von Tracking- und vorgangsbedingten Daten ernsthaft privatheitsfreundlich angegangen würden, zumal dies Fachwissen und einen guten Überblick über den Datenbestand – insbesondere jenseits einzelner Kampagnen – erfordert.

Bürger, Unternehmen und öffentliche Institutionen sachlich und umfassend bzgl. Tracking und möglichen Gegenmaßnahmen informieren und sensibilisieren.

Über die Möglichkeiten des Internettrackings, die dadurch gewinnbaren Daten sowie zur privatheitsfreundlichen Gestaltung von Online-Angeboten und zum Selbstschutz von Internetnutzern besteht erheblicher Informationsbedarf. Ein Teil der kursierenden Informationen ist unsachlich verharmlosend oder schwarzmalerisch, was aber für die Nutzer nicht unbedingt erkennbar ist. Deshalb bedarf es sachlicher, leicht verständlicher Informationen von neutraler Seite. Bei klar kategorisierbaren Sachverhalten könnten dazu auch staatlich anerkannte (Qualitäts-)Siegel eingesetzt werden.

GLOSSAR

Account: Mitglieds- oder Nutzerkonto.

Anwendungsinstanz: Eine aktive Kopie einer Anwendung. Eine Anwendungsinstanz existiert zwischen dem Starten und dem Beenden einer Anwendung. Bei vielen Anwendungen ist auf einem Gerät immer nur eine aktive Kopie möglich, ein erneuter Start, während eine aktive Kopie existiert, führt dann z. B. nur zu einem zusätzlichen Fenster.

Browser-Add-on: Browsererweiterung, die auf dem Rechner des Nutzers installiert werdenkann; typischerweise von Dritten bereitgestellt. Add-ons können die Privatheit der Nutzer erhöhen, aber auch selbst Tracking ermöglichen.

Browsertab (oder kurz: Tab): Registerkarte, Reiter.

Cookie: Kleiner, auf dem Gerät des Nutzers gespeicherter Datensatz. Wir subsumieren unter dem Begriff »Cookies« alle Formen von verlaufs- oder verhaltensbezogenen Daten, die bei der Internetnutzung auf dem Gerät des Nutzers gespeichert werden und von lokalem Code (vor allem JavaScript) weiterverwendet werden können oder beim erneuten Kontaktieren der speichernden Domäne mitgeschickt werden. Technisch gehören dazu z. B. auch sogenannte Super Cookies, Flash Cookies, LSO Cookies und Inhalte des DOM Storage. Standard-Cookies werden automatisch bei Abruf eines Webelementes der entsprechenden Domäne mitgeschickt und ggf. aktualisiert, auch wenn JavaScript abgeschaltet ist. Die anderen Cookie-Typen benötigen JavaScript für die lokale Verwaltung auf dem Nutzergerät und die Kommunikation mit der zuständigen Domäne. Sie können über die Standard-Benutzeroberfläche des Browsers nicht individuell verwaltet (gelöscht) werden.

Demand Side (Nachfragerseite): Hier Die Werbenden.

Dienstanbieter: Online-Anbieter, Internetanbieter oder Telekommunikations-Dienstanbieter.

»digitaler Schatten«: Gesichts- und namenloses Objekt, das anhand seiner Eigenschaften, Vorlieben, Verhaltensweisen … eindeutig wiedererkennbar ist. Internettracking strebt an, das zwischen digitalen Schatten und realen Personen eine 1-zu-1-Beziehung besteht.

Domäne: Im Kontext dieses Dokumentes: Website.

Domänenname: Z. B. »online-anbieter.de«, »trackingdomaene.com« ... der gemeinsame Adressteil aller Webelemente einer Website.

Domänensitzung: Allgemein: Die Zeit, in der ununterbrochen mindestens eine Webseite einer gegebenen Domäne innerhalb derselben Browserinstanz (s. Abschnitt 4) oder derselben App genutzt wird (entsprechender/s Tab bzw. Fenster vorhanden). Spezieller: Die Zeit zwischen einem Login und dem zugehörigen Logout.

Drittanbieter: Werden von Code angesprochen, der in Webelementen enthalten ist und (weitere) Webelemente abruft. Beim automatischen, auch mittelbaren Abruf aus Webseiten heraus: Die Bereitsteller von Webelementen, die nicht mit dem (Erst-)Anbieter der umgebenden Webseite identisch sind. Trackingdienstleister sind typischerweise Drittanbieter.

Echokammer: S. Filterblase.

Ende-zu-Ende-Verschlüsselung: Die Verschlüsselung erfolgt mit einem adressatenspezifischen Schlüssel. Ist dieser nur den Kommunikationspartnern ekannt, können beteiligte Online-Anbietr die verschlüsselten Inhalte nicht auswerten.

Erstanbieter: Die Betreiber von Websites, von denen der Nutzer *explizit* (oder mittels browserextern angeklickter Links) vornehmlich Webseiten (aber auch andere Webelemente) abruft.

Filterblase: Dem Nutzer werden nur oder vornehmlich Web-Inhalte präsentiert, die seine Vorlieben reflektieren und seine Meinungen bestärken. So wird versucht, die Verweildauer des Nutzers auf den entsprechenden Websites zu erhöhen, z. B. um ihm mehr Werbung präsentieren zu können.

Formaler Anbieter eines Online-Angebotes: Als formaler Anbieter eines Online-Angebotes wird im Rahmen dieses Dokumentes aus praktischen Erwägungen der Dienstleister betrachtet, der inhaltlich verantwortlich für den Dienst ist und unter dessen Domänennamen das Angebot bereitgestellt wird. Typischerweise ist dieser auch der Besitzer des Domänennamens und im Impressum des Online-Angebotes genannt.

Funktionaler Betreiber eines Online-Angebotes: Funktionaler Betreiber eines Online Angebotes ist der Dienstleister, der das Angebot technisch zur Verfügung stellt. Er kann mit dem Anbieter identisch oder im Auftrag des Anbieters tätig sein. Auf funktionale Betreiber wird in diesem Dokument nur am Rande, z. B. im Zusammenhang mit Content Delivery Networks (s. Abschnitt 3.4), eingegangen. Sie spielen im Zusammenhang mit Tracking eine untergeordnete Rolle.

Geotracking: Die Aufzeichnung der Position bzw. des Weges eines Objektes, z. B. einer Person oder eines Fahrzeugs.

GPS-Empfänger: Funkempfänger zum Empfang von Signalen, die die eigene Positionsbestimmung ermöglichen.

Hash-Wert: Durch eine Einweg-Funktion aus einer ursprünglichen Zeichenkette – z. B. einem Namen – gewonnene Zeichenkette, die sich nur mit sehr großem Aufwand in die ursprüngliche Zeichenkette zurückverwandeln lässt. Kennt jemand jedoch die ursprüngliche Zeichenkette, kann er den Hash-Wert ebenfalls berechnen und anschließend in beliebigen Daten wiedererkennen.

IMEI: International Mobile Equipment Identity; eindeutiger Identifikator jedes Mobilfunkgerätes.

Individualisierte Werbung: In der Literatur wird diese Art der Werbungsauswahl meist als »verhaltensbasierte Werbung« bezeichnet (englisch »Behavioral Advertising« oder »Behavioral Targeting«). Da dieser Begriff nicht offensichtlich auch auf z. B. aus sozialen Netzen gewonnene Informationen hindeutet und für Laien nicht klar vom Begriff »kontextbasierte Werbung« (Werbung auf der Basis der aktuell konsumierten Online-Angebote) abgegrenzt ist, wurde hier die Bezeichnung »individualisierte Werbung« gewählt.

Individualisierung: Im Kontext dieses Dokumentes: Internetinhalte oder Werbung, die Nutzern nur bei (angenommenem) Vorliegen bestimmter Nutzereigenschaften präsentiert werden oder die verschiedenen Nutzern in Abhängigkeit von deren Eigenschaften unterschiedlich präsentiert werden.

Informationsfreiheit: In diesem Dokument wird der weiter gefasste Begriff zugrunde gelegt, der nicht nur Daten der öffentlichen Hand umfasst.

Inhaltsdaten: Daten, die der Nutzer eingibt oder online konsumiert.

Instant Messaging: Nachrichtensofortversand; in der Basisfunktionalität ähnlich SMS, meist aber mit erweiterten Möglichkeiten zum Versand von Bildern, Tonaufnahmen …

Intelligenter digitaler Assistent: Beispiele: Alexa/Echo, Siri, Cortana, Google Assistent; erfasst natürliche Sprache, wertet diese semantisch/syntaktisch aus und reagiert, beispielsweise indem er Fragen beantwortet oder einfache Aufträge ausführt.

»Internet-Beschleuniger«: Beispiele: Facebook Instant Articles, Google AMP. Als Internet-Beschleuniger werden unterschiedliche Konzepte bezeichnet, die insbesondere das Laden komplexer Webseiten auf leistungsschwachen oder mit geringer Datenrate angebundenen Geräten beschleunigen sollen. Dazu gehören z. B. Dienste, die Bilder zentral herunterskalieren, um den Download zu beschleunigen, und Dienste, die bestimmte Webelemente zentral bereithalten, um Wartezeiten zu verringern.

Internetanbieter, Internet-Dienstanbieter (Internet Service Provider, ISP): Allgemein: Ein Dienstleister, der Daten durch das Internet transportiert.
Speziell: (Kommerzieller) Anbieter und Betreiber von Internetanschlüssen; auch als Internet-Anschlussbetreiber bezeichnet. (S. auch J. Tiemann, G. Goldacker: »Vernetzung als Infrastruktur – ein Internet-Modell«, Kompetenzzentrum Öffentliche IT, Fraunhofer FOKUS, 1. Auflage, Oktober 2015, https://www.oeffentliche-it.de/documents/10181/14412/Vernetzung+als+Infrastruktur+-+Ein+Internet-Modell.)

IP-Adresse: Die Adresse, unter der ein Gerät (Endgerät oder Router) im Internet erreichbar ist. Diese sollte weder mit einer Webadresse noch mit einem Domänennamen verwechselt werden. Eine IP-Adresse ist – abhängig vom benutzten Kommunikationsprotokoll – 4 Bytes (bei IPv4) bzw. 16 Bytes (bei IPv6) lang.

Klient: Nutzerseitiges Programm, das für die Kommunikation, z. B. mittels E-Mail oder Instant Messaging, genutzt wird.

Kommunikationsprotokoll: Eine »Sprache«, mit der Programme z. B. über das Internet Daten miteinander austauschen.

Leitungsverschlüsselung: Leitungsverschlüsselung findet nicht unbedingt direkt zwischen Kommunikationspartnern, sondern typischerweise abschnittsweise (»pro Leitung«) zwischen den Nutzern und ihren Online-Anbietern bzw. zwischen verschiedenen Online-Anbietern statt. Bei jedem beteiligten Online Anbieter liegt die Kommunikation zumindest zeitweilig unverschlüsselt vor und kann von diesem inhaltlich ausgewertet werden. Dieses Verfahren ist z. B. bei E-Mail und Instant Messaging weit verbreitet und schützt lediglich gegen die Auswertung durch Dritte.

»Liken«: Seine Zustimmung zu einem Webinhalt o. Ä. durch Klicken eines entsprechenden elektronischen »Buttons« (»Knopfes«) auf einer Webseite kundtun.

Link, Weblink: Webadresse, vornehmlich wenn sie z. B. in einer Webseite, einer E-Mail oder einer Lesezeichenliste enthalten ist und automatisch oder durch Klicken des Nutzers das entsprechende Webelement heruntergeladen wird. Auch wenn der Nutzer z. B. auf ein Wort, eine Textpassage oder ein Bild klicken kann, verbirgt sich dahinter stets eine Webadresse, die alle in Abschnitt 5.4 beschriebenen Elemente enthalten kann.

Logdaten: Generell: Alle Daten, die zu in einem gegebenen Kontext beobachteten Ereignissen aufgezeichnet werden. Speziell: Z. B. Ein- und Ausschaltereignisse von Geräten (mit Zeitangaben).

Login-Sitzung: Zeitspanne zwischen Login und explizitem (durch Nutzereingabe), implizitem (z. B. durch Zeitablauf) oder forciertem (z. B. durch Abbruch der Browserinstanz) Logout.

Nebengeordnete Subdomäne: Subdomäne in einem anderen Strukturpfad derselben Domäne, z. B. »www.online-anbieter.de« und »tracking.online-anbieter.de«.

Nutzungserlebnis (»User Experience«): (Subjektives) Empfinden bei der Nutzung (z. B. einer Webseite).

Online-Anbieter (Online-Dienstanbieter): S. formaler Anbieter eines Online-Angebotes.

Online-Dienst: Im Gegensatz zu Transportdienstleistungen, wie sie von Internet-Dienstanbietern erbracht werden, gehören zu den Online-Diensten z. B. die Bereitstellung von Informationen (Nachrichten, Suchergebnissen) und Medien (Audio- und Videodownload und -streaming) sowie komplexere Telekommunikationsdienste (Internettelefonie, Messenger).

Over-the-Top-Dienst (OTT-Dienst): Dienst, der von einem Dritten unter Nutzung von Internet- oder Telekommunikationsnetz-Basisinfrastrukturen erbracht wird.

Persona: Im Kontext dieses Dokumentes: Nutzerkategorie. Jeder Internetnutzer wird anhand seiner bekannten oder aus Beobachtungen geschlossenen Eigenschaften, Vorlieben … für jede Situation, in der eine Entscheidung bzgl. des Nutzers getroffen wird (z. B. über eine Werbeeinblendung), einer situationsabhängigen Persona zugeordnet. Personas können sehr allgemein gehalten sein (männlich/weiblich) oder einen hohen Detailgrad aufweisen. Je höher der Detailgrad, desto mehr Personas kommen prinzipiell infrage, weshalb die Wahl eines geeigneten Detailgrades ein Optimierungsproblem darstellt.

Personalisierung: Im Kontext dieses Dokumentes: Links, Webseitenadressen, Internetinhalte, Werbung … die individuelle personenbezogene Daten wie Name, Adresse, E-Mail-Adresse … enthalten.

Referrer (engl.), »Referer«: Verweiser, der die aufrufende Webseitenadresse enthält; fachsprachlich hat sich die fehlerhafte Schreibweise »Referer« durchgesetzt.

Session: Dieser Begriff, zu Deutsch »Sitzung«, wird semantisch nicht eindeutig benutzt, siehe z. B. der unterschiedliche Sessionbegriff bei Browsersessions und der Session ID.

Session ID: Sitzungsbezeichner, Beispiel: »http://www.beispieldomaene.de/index.html?*jsessionid=abcde12345*«.

Subdomäne: Unterstruktur einer Website.

Subdomänenname: Z. B. »count.trackingdomaene.de«, spezieller Domänenname, der eine Subdomäne adressiert.

Supply Side (Anbieterseite): Hier: Die Anbieter von Online-Diensten, in deren Angebote Werbung eingeblendet wird.

Targeting: Die auf einzelne Nutzer (oder kleine Gruppen von Nutzern) bezogene Auswahl von Werbeeinblendungen, politischen Botschaften … anhand von Nutzereigenschaften/-vorlieben oder des Nutzungskontextes (Ort, Zeit …).

Usability: (Objektive) Nutz- und Bedienbarkeit (z. B. einer Webseite).

Verhaltensdaten: Beispiel: Reagiert der Nutzer sofort oder erst nach mehrmaliger Wiederholung (einer Werbung, einer Betrachtung eines online angebotenen Artikels …)?

Verlaufsdaten, Verkehrsdaten: Wann und wie lange fand welche Aktivität statt?

Webadresse: Eine Webadresse (URL: Uniform Resource Locator) besteht typischerweise aus der Angabe des zu verwendenden Kommunikationsprotokolls (»HTTPS« oder »HTTP«), dem Domänennamen des Online-Anbieters und den Angaben, die die Bestimmung des auszuliefernden Webelementes ermöglichen. Beispiele:
»http://www.beispieldomaene.de/start.html« (Webseite),
»https://images.beispieldomaene2.de/bild.jpg«,
»http://www.beispieldomaene3/dokument.pdf«.
Webadressen können individualisiert oder personalisiert sein.

Webdomäne (oder kurz: Domäne): Im Kontext dieses Dokumentes: Website.

Webelemente: Webseiten, Bilder, Videos, ergänzender Webseitencode, Daten für die Gestaltung der Webseitenanzeige … bis hin zu komplexen, dynamischen Objekten, die mit Web-Kommunikationsprotokollen heruntergeladen und innerhalb oder außerhalb eines Browsers angezeigt werden. Webseiten, E-Mails, PDF-Dokumente … können Code enthalten, der das Herunterladen weiterer Webelemente, auch von anderen Websites, veranlasst. Werbung beispielsweise ist oft nicht direkt in die umgebende Webseite eingebettet, sondern wird als externes Webelement hinzugeladen.

Webseite: Das nach einem Webabruf über eine Adresseingabe oder das Anklicken eines Links in einem Browser angezeigte Hauptdokument mit allen ggf. ergänzend heruntergeladenen Webelementen. Die eingegebene oder angeklickte Adresse bezieht sich auf das Hauptdokument.

Webserver: Der technische Lieferant eines Webelementes.

Website: Die Gesamtheit aller Webelemente, die von einem Anbieter unter einem Domänennamen bereitgestellt wird.

Werbe-ID: Engl. Ad-ID oder Identifier for Advertisers (IDFA); ein spezieller, dauerhafter Identifikator für Mobilgeräte, der insbesondere für die Nutzung durch die Werbebranche vorgesehen ist. Die Werbe-ID kann vom Nutzer geändert werden.

Zählpixel: Weitere verbreitete Bezeichnungen: Tracking Pixel, Web-Bug, Web-Beacon; winzige, meist völlig durchsichtige und farblose »Bilder«, die vom Betrachter einer Webseite in der Regel nicht bemerkt werden.

Zustandsdaten: Z. B.: Welcher Browser, welches Betriebssystem wird benutzt?

KONTAKT

Gabriele Goldacker
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de
Twitter: @OeffentlicheIT

ISBN: 978-3-9818892-6-0

kre | 1809 (Fotos: https://pixabay.com/; Infografiken: ÖFIT)