WHITEPAPER

BVDW
Wir sind das Netz

Browsercookies und alternative Tracking-Technologien:
technische und datenschutzrechtliche Aspekte

Inhaltsübersicht

RECHT
RESSORT IM BVDW

TARGETING
FOKUSGRUPPE IM BVDW

1. Einleitung

Im Internet versteht man unter Tracking die quantitative Messung und das Nachvollziehen des Nutzerverhaltens auf Websites sowie in einem weiteren Nutzungskontext die Messung von Werbeeinblendungen zum Zweck der Auslieferungskontrolle und -steuerung. Ein verlässlich funktionierendes Tracking, das eindeutige Ergebnisse über alle benötigten Metriken liefert und zugleich eine optimale Aussteuerung erlaubt, ist für Webangebote und werbetreibende Unternehmen im heute bestehenden wirtschaftlichen Konkurrenzumfeld absolut unerlässlich. Den technologischen Schlüssel zu einem leistungsfähigen Tracking liefert bis heute das Browsercookie, das häufig auch einfach nur als „Cookie" bezeichnet wird. Daher widmet sich das Whitepaper dieser Technologie zu Beginn ausführlich.

Zugleich beobachtet der Bundesverband Digitale Wirtschaft (BVDW) e.V. auch, dass die Bedeutung des Cookies, vor allem des sogenannten Third-Party-Cookies, als zentrales Element der Tracking-Technologien im Internet im Abnehmen begriffen ist. Die Gründe hierfür liegen vor allem in der sinkenden Cookie-Akzeptanz der Internetnutzer und in Änderungen im Default-Cookie-Handling bei einigen Browsern und Betriebssystemen mit relevanten Marktanteilen. Diese akzeptieren Cookies von Drittparteien (Third-Party-Cookie) – wozu die Cookies nahezu aller Tracking-Systeme zählen – nicht mehr als Voreinstellung bei Inbetriebnahme. Das führt dazu, dass Alternativen zum Browsercookie zunehmend in den Fokus der Aufmerksamkeit geraten. Hier haben sich neue Technologien etabliert, welche die Verwendung von Cookies in Zukunft ergänzen oder überflüssig machen können. Viele der Verfahren sind schon seit Jahren bekannt, wurden aber bisher kaum eingesetzt.

In diesem Whitepaper informiert die Fokusgruppe Targeting zusammen mit dem Ressort Recht im BVDW über die aktuellen technischen Entwicklungen im Bereich Tracking und gibt einen Überblick zur rechtlichen Einordnung von Cookies sowie alternativen Technologien. Zielgruppe ist hierbei zum einen die gesamte Onlinebranche, die im Einsatz über die aktuellen technischen Entwicklungen und datenschutzrechtlichen Gegebenheiten informiert werden soll, aber zum anderen auch die politische Sphäre, deren Entscheidungen maßgeblich die wirtschaftlichen Entwicklungen in diesem Bereich beeinflussen. Ziel ist, allen partizipierenden Marktteilnehmern aufzuzeigen, in welcher Form alternative Tracking-Technologien unter Beachtung möglich technologischer und auch datenschutzrechtlicher Restriktionen und im Vergleich zur heute noch weitverbreiteten Technologie des Browsercookies eingesetzt werden können.

2. Tracking und Datenschutz

Wo immer automatisierte Verarbeitungen von Daten im Zusammenhang mit der Nutzung oder Offenlegung von Identitäten oder Handlungen einer Person erfolgen, stellt sich die Frage nach den rechtlichen Handlungsspielräumen der verarbeitenden Stelle aus datenschutzrechtlicher Sicht.

2.1. Personenbezogene Daten

Die Vorgaben des Datenschutzrechts sind grundsätzlich nur dann zu beachten, wenn es sich bei den verarbeiteten Daten tatsächlich um „personenbezogene" Daten handelt. Nach der Definition des Bundesdatenschutzgesetzes (BDSG) sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (§ 3 Abs. 1 BDSG). Gemeint sind damit Daten, durch die man eine

Person unschwer identifizieren kann – wie zum Beispiel Name, Adresse, Telefonnummer, persönliche E-Mail-Adresse.

Unter dem Begriff „personenbezogen" sollen nach Ansicht der Datenschutzbehörden[1] allerdings auch andere Daten fallen, wie die IP-Adresse, eindeutige Gerätekennungen (IMEI/International Mobile Equipment Identity; UDID/Unique Device Identifier sowie MAC/Media Access Control) sowie Standortdaten oder Informationen über die Nutzung von Apps auf einem Endgerät. In vielen Fällen, wie bei der IP-Adresse, ist diese strikte Einordnung allerdings zweifelhaft und – anders als häufig dargestellt – nicht unumstritten. So stellen dynamische IP-Adressen keine personenbezogenen Daten im Sinne von §§ 12 TMG, 3 BDSG dar, soweit der Betreiber einer Website diese ohne den dazugehörigen Zeitpunkt des Zugriffs speichert[2]. Auch bei Speicherung des Zugriffszeitpunktes ist Personenbezogenheit nur anzunehmen, wenn dem Anbieter die Bestimmung der Person des Nutzers technisch und rechtlich möglich ist. Dies dürfte bei Tracking-Anbietern im Grunde nie der Fall sein.

Soweit das Gesetz nicht eine eigene Erlaubnis vorsieht (z.B. bei Verwendung der Lieferanschrift und Zahlungsdaten), bedarf jede anderweitige Nutzung personenbezogener Daten (das Gesetz spricht von „Erhebung, Verarbeitung und Nutzung") der Einwilligung der betroffenen Person. Dies gilt insbesondere hinsichtlich der Verwendung für Zwecke der Werbung oder Marktforschung. Wer also solche (Klar-) Daten im Rahmen der Erstellung eines Nutzerprofils erfasst, bedarf für die weitere Verwendung grundsätzlich der Zustimmung der betroffenen Person. Das gilt auch für die Anreicherung oder Verknüpfung solcher Profile mit personenbezogenen Daten. Eine Ausnahme besteht hier lediglich für die Verwendung von Adressdaten bei postalischer Werbung (Listendatenprivileg).

Der Vollständigkeit halber sei erwähnt, dass das BDSG „besondere Arten" von personenbezogenen Daten kennt (§ 3 Abs. 9 BDSG). Das sind herausgehoben schützenswerte Angaben über die rassische oder ethnische Herkunft, die politische Meinung, religiöse oder philosophische/weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder das Sexualleben. Wer solche Daten erhebt, muss besondere, vor allem formale Voraussetzungen für ihre Nutzung erfüllen, zum Beispiel sind für die Schriftform von Einwilligungserklärungen besondere Kriterien zu erfüllen.

2.2. Nutzungsdaten

Für den Online-Bereich enthält das Telemediengesetz eigene Regeln zum Umgang mit personenbezogenen Daten. Auch hier stellt das Gesetz zunächst klar, dass personenbezogene Daten ohne Einwilligung erhoben und genutzt werden dürfen, wenn entweder eine Einwilligung des Nutzers vorliegt oder eine gesetzliche Erlaubnis besteht (§ 12 TMG). Dies betrifft in erster Linie die Bestandsdaten, also Daten, die für die Begründung, Ausgestaltung oder Änderung eines Vertragsverhältnisses erforderlich sind – gemeint sind zum Beispiel die klassischen CRM-Daten (Customer-Relationship-Management), dazu gehören wie schon erwähnt auch Vertragsdaten. Daher ist hier die gesetzliche Regelung für Online-Daten zunächst nicht anders als bei Offline-Daten.

[1] Vgl. Düsseldorfer Kreis: Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, 16. Juni 2014
[2] LG Berlin, 31.01.2013, Az.: 57 S 87/08

Gesetzlich erlaubt ist die Nutzung weiterer, als personenbezogen geltende Daten auch dann, wenn diese erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Das Gesetz spricht in diesem Falle von Nutzungsdaten und zählt dazu insbesondere Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien (§ 15 TMG).

Anders als in der analogen Welt dürfen digitale Nutzungsdaten zum Zwecke der Werbung oder Marktforschung aber dann einwilligungslos in Nutzungsprofilen Verarbeitung finden, wenn diese unter Verwendung von Pseudonymen erstellt werden (§ 15 Abs.3 TMG). Eine weltweit fast einzigartige Vorschrift. Es ist daher schwer nachvollziehbar, warum IP-Adressen oder Gerätekennungen nach Ansicht der Datenschutzbehörden einerseits Nutzungsdaten sein sollen, diese jedoch nicht in pseudonymen Nutzerprofilen gespeichert werden dürfen, da sie selbst kein Pseudonym darstellen sollen.[3]

2.3. Pseudonyme Daten

Pseudonyme Daten liegen vor, wenn der Name oder andere Identifikationsmerkmale durch ein Pseudonym ersetzt wurden, z.B. durch eine Kennziffer. Das gilt aber nur dann, wenn die Pseudonymisierung reversibel ist, das Pseudonym also wieder aufgelöst werden kann, z.B. durch den Inhaber einer Zuordnungstabelle oder schlicht den Inhaber des „Schlüssels", der die Pseudonymisierung herbeiführte. Ein typisches Beispiel ist die Nutzer-ID in einem Cookie. Sie kann ein Pseudonym darstellen, wenn es einen Schlüssel gibt, der es dem Inhaber dieses Schüssels ermöglicht, die Daten zu entpseudonymisieren.

Können pseudonymisierte Daten nicht mehr aufgelöst werden, sind sie irreversibel. In diesem Fall liegen keine pseudonymen Daten mehr vor, sondern anonyme Daten. Auch für denjenigen, der nicht im Besitz des Schlüssels ist, stellen sich pseudonyme Daten bei genauerer Betrachtung als anonyme Daten dar.

2.4. Anonyme Daten

Anonyme Daten liegen vor, wenn personenbezogene Daten so verändert wurden, dass die Einzelangaben nicht mehr oder nur mit unverhältnismäßig großem Aufwand „an Zeit, Kosten oder Arbeitskraft" einer bestimmten oder bestimmbaren Person zugeordnet werden können (§ 3 Abs. 6 BDSG). Insbesondere der Begriff der „bestimmbaren Person" löst in der Praxis heftige Diskussionen aus. Kommt es für diese Frage auf die Sicht des konkreten Anwenders an (also eine relative Sicht), oder ist eine objektive Betrachtungsweise die richtige?

Die Relevanz dieser Frage wird zum Beispiel bei IP-Adressen deutlich. Für einen Zugangsprovider, z.B. die Deutsche Telekom, ist der Inhaber einer IP-Adresse bestimmbar. Der Vermarkter einer Website ist dagegen nicht ohne Weiteres in der Lage, die hinter einer IP-Adresse stehende Person zu ermitteln. Käme es auf die objektive Betrachtungsweise an, würde es ausreichen, dass irgendwer auf dieser Welt in der Lage wäre, eine IP-Adresse aufzulösen. Kommt es dagegen auf die relative Sicht an, wäre die Erfassung einer IP-Adresse durch einen Vermarkter datenschutzrechtlich zulässig. Die Rechtsprechung ist unentschieden, der Bundesgerichtshof (BGH) hat diese Frage dem Europäischen Gerichtshof (EuGH) vorgelegt. Er

[3] Vgl. Düsseldorfer Kreis: Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, 16. Juni 2014, S. 11

scheint aber der relativen Sichtweise zuzuneigen. Es bleibt daher abzuwarten, wie der EuGH in dieser für die Online-Branche äußerst wichtigen Frage entscheidet.

Das besondere an anonymen Daten ist der Umstand, dass die Datenschutzgesetze für sie nicht gelten. Die Nutzung und Verarbeitung von anonymen Daten ist gesetzlich praktisch nicht geregelt. Sie bedarf insbesondere keiner Einwilligung eines Betroffenen, denn es gibt in diesem Fall niemanden, der sich betroffen fühlen kann. Der Umstand, dass eine Verarbeitung von anonymen Daten praktisch grenzenlos möglich ist, hat für die Onlinebranche eine wesentliche Bedeutung. Denn in der Regel erfordert der Einsatz von Tracking-Technologien nicht die Nutzung personenbezogener Daten. Die Verarbeitung anonymer Kennziffern und Nutzerprofile, die einen Rückschluss auf die dahinterstehende Person nicht zulassen, reicht in der Regel aus.

Das Anonymisieren eines personenbezogenen Datums ist übrigens nicht zustimmungsbedürftig. Wer also seine in der CRM vorhandenen Kundendatenbestände anonymisiert und anschließend mit (anonymen) Offlineprofilen „matcht", benötigt häufig keine Einwilligung der betroffenen Nutzer. Natürlich kommt es dabei sehr auf den konkreten Einzelfall an. Die Anonymisierung muss auch nicht durch einen Dritten erfolgen, zum Beispiel einen externen Anonymizer, auch wenn das im Sinne einer „informationellen Gewaltenteilung" durchaus wünschenswert erscheinen mag. Allein maßgeblich ist sicherzustellen, dass jede Re-Identifizierung technisch endgültig ausgeschlossen bleibt.

2.5. Praktische Relevanz der Unterscheidung

Die Unterscheidung insbesondere zwischen personenbezogenen und anonymen Daten ist von kaum zu überschätzender Bedeutung für die Onlinebranche. Wer personenbezogene Daten erhebt, braucht in der Regel die vorherige Einwilligung des Nutzers. Wer dagegen anonyme Daten verarbeitet, fällt nicht (mehr) unter die Vorgaben des Datenschutzrechts.

Die Frage, ob eine Tracking-Technologie zur Verarbeitung von personenbezogenen Daten führt, ist daher für ihren rechtlich zulässigen Einsatz entscheidend. Greift die jeweilige Technologie nur auf anonyme Daten zurück, ist ihr Einsatz ohne Zustimmung eines Nutzers zulässig; werden dagegen personenbezogene Daten verarbeitet oder kommt es auch nur zur Anreicherung anonymer Daten mit personenbezogenen Daten (z.B. beim Hinzuspeichern von E-Mail-Adressen zu einem anonymen Nutzerprofil), bedarf dies der Zustimmung.

Es muss daher das Ziel jedes Geschäftsmodells in der Onlinebranche sein, mit anonymen Daten zu arbeiten, jedenfalls dort, wo es sinnvoll ist, und das ist insbesondere beim Tracking der Fall.

3. Browser-Cookies

Zu der derzeit verbreitetsten Tracking-Methode zählt zweifelsohne noch immer die Verarbeitung von aus Cookies gewonnenen Daten. Im allgemeinen Sprachgebrauch wird als Bezeichnung des Browser-Cookies häufig nur das Wort „Cookie" gebraucht. Unter dem Begriff Browser-Cookies werden einfache Textdateien verstanden, die auf dem Endgerät eines Nutzers (z.B. Computer, Tablet, Smartphone) abgelegt werden und die Wiedererkennung des Nutzers ermöglichen. Ein Browser-Cookie wird dazu entweder vom Webserver an den Browser gesendet oder von einem Skript (etwa JavaScript) in der Website erzeugt.

Ohne Browser-Cookies wären heute viele übliche Nutzungshandlungen im Internet nahezu undenkbar, da das Internet-Protokoll „http" aufgrund seiner Zustandslosigkeit selbst keinen Austausch von Daten aus unterschiedlichen Serveranfragen ermöglicht. Ist eine Serveranfrage (Website-Aufruf) abgeschlossen, wird die Interaktion vergessen. Das Protokoll kann sich keine weiteren Informationen „merken". Über Browser-Cookies können jedoch Daten über mehrere Verbindungen (Sitzungen) hinweg gespeichert werden. Beim Ansteuern einer Website liest der jeweilige Dienst bereits existierende Cookies aus oder platziert selbst ein Cookie, das die benötigten Informationen bei künftigen Aufrufen der Website bereitstellt. Somit kann der Nutzer zum Beispiel auch beim nächsten Website-Besuch dieselbe Ansicht der Website vorfinden, die er in einer vorherigen Sitzung gewählt hat. Er muss sich nicht bei jedem Besuch neu einloggen, seine Merklisten und Warenkörbe können erhalten bleiben, weil er wiedererkannt wird.

Browser-Cookies können mit jeder übermittelten Datei übertragen werden, also auch mit Bilddateien wie zum Beispiel Werbebannern oder jedem anderen Dateityp. Welche Cookies im Browser gespeichert sind, lässt sich über die Datenschutzeinstellungen im Browser herausfinden.

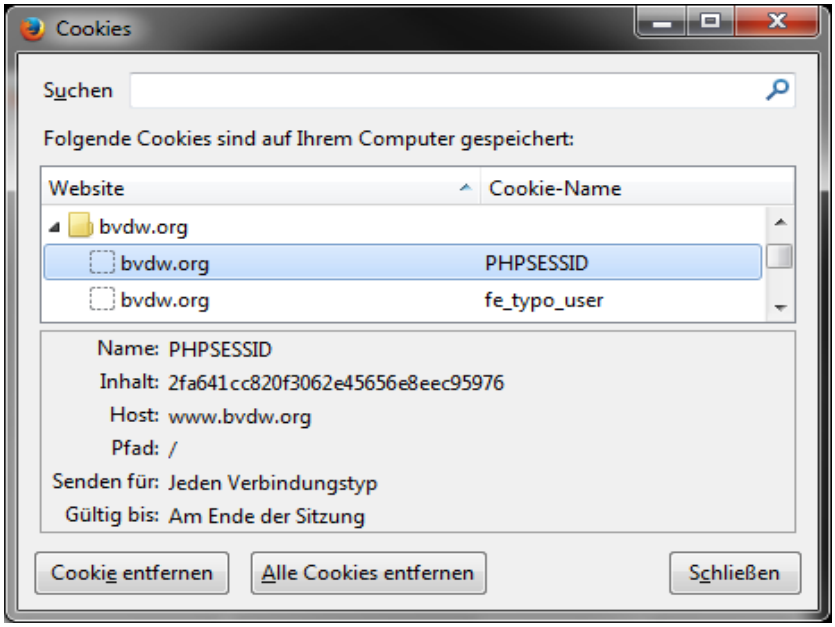

Abb.: Datenschutzeinstellungen des Browsers Mozilla Firefox

3.1. First- und Third-Party-Cookies

Wird ein Browser-Cookie von der Domain der Website, auf der sich ein Internetnutzer gerade aufhält, gesetzt, so nennt man dies ein First-Party-Cookie. Alle Cookies, die dem Nutzer von anderen Domains gesetzt werden, als jener, die oben in der URL-Zeile des Browsers erscheint, nennt man Third-Party-Cookies. Dabei handelt es sich also um Cookies von Domains, die ein Nutzer nicht wissentlich angesteuert hat, die aber Bestandteile des Inhalts anliefern, zum Beispiel spezielle Inhalte oder Werbebanner, die im Browserfenster zu sehen sind.

Technisch und in den Nutzungsmöglichkeiten gibt es zwischen First- und Third-Party-Cookies keinerlei Unterschiede. Über die Datenschutzeinstellungen im Browser kann aber der Umgang mit den beiden Typen des Browser-Cookies unterschiedlich geregelt werden.

3.2. Einsatz von Browser-Cookies zur Messung, Steuerung und Profilbildung

Browser-Cookies sind heute noch das am häufigsten genutzte Instrument, um in Online-Werbekampagnen eine Wiedererkennung eines Browsers herbeizuführen und damit Kampagnenerfolge zu messen, die Zahl der Werbeeinblendungen pro Nutzer zu regulieren und Profile für verhaltensbasierte Werbeeinblendungen zu erstellen. Prinzipiell ist hierbei zwischen zwei Vorgehensweisen zu unterscheiden.

Beim ersten Verfahren werden die zu speichernden Inhalte direkt im Cookie, also in der Textdatei auf dem Rechner des Nutzers abgelegt. Dies hat den Vorteil eines schnellen Zugriffs direkt auf dem Endgerät und spart auf dem Webserver Ressourcen. Allerdings können in einem Browser-Cookie direkt nur eine stark begrenzte Menge von Daten gespeichert werden, je nach Hersteller sind es maximal vier Kilobyte. Deshalb nutzen die meisten Tracking-Systeme eine alternative Vorgehensweise, bei der im Browser-Cookie selbst nur eine eindeutige Laufnummer (Nutzer-ID) abgelegt und die zugehörigen Profilinhalte auf dem Webserver gespeichert werden.

Der Internetnutzer hat bei Browser-Cookies die Möglichkeit, sich über die Bedienoberfläche des Programms anzeigen zu lassen, welche Websites auf seinem Rechner Cookies abgelegt haben und sich den Inhalt der Cookies anzeigen lassen. Die gespeicherten Cookies kann er dann nach Wunsch einzeln oder komplett löschen.

Über die Datenschutzeinstellungen des Browsers kann der Nutzer zudem den Umgang mit Browser-Cookies für zukünftige Internet-Sitzungen (Session) differenziert einstellen. Die Einstellungsmöglichkeiten unterscheiden sich im Detail je nach Browserprodukt, bieten aber immer die Möglichkeit festzulegen, ob Cookies gar nicht akzeptiert werden, nur für die Laufzeit der Session, also bis zum Schließen des Programms, oder dauerhaft gespeichert werden sollen. Hierbei können für First-Party- und Third-Party-Cookies unterschiedliche Einstellungen vorgenommen werden.

In den Voreinstellungen (Default-Einstellungen) für das Cookie-Handling unterscheiden sich die marktüblichen Browser beim Umgang mit Third-Party-Cookies. Diese werden von Apple Safari standardmäßig nicht gespeichert, die anderen Produkte mit relevantem Marktanteil, wie Microsoft Internet Explorer, Mozilla Firefox oder Google Chrome, akzeptieren sie dagegen genauso wie die First-Party-Cookies.

3.3. Cookies und Datenschutz

Mithilfe von Cookies können – wie dargestellt – sowohl die Website-Betreiber selbst (first party) als auch dritte Anbieter (third party) sehr unterschiedliche Informationen, wie Browsertyp oder Spracheinstellungen, aber auch Website-Besuche, über einen bestimmten Nutzungszeitraum hinweg sammeln und speichern. Nicht in allen Fällen weisen diese Daten Personenbezug auf. Wo allerdings Nutzungsdaten mit personenbezogenen Informationen anfallen, gelten zur Verarbeitung die Vorgaben des deutschen Datenschutzrechts.

3.3.1. Datenschutzrechtliche Regelungen im Telemediengesetz (TMG)

Eine Regelung im deutschen Telemediengesetz, die sich ausdrücklich auf Cookies bezieht, gibt es nicht. Allerdings muss ein Website-Betreiber die Nutzer über den Einsatz von Verfahren informieren, bei denen personenbezogene Daten erhoben und verarbeitet werden. Diese Informationspflichten des Diensteanbieters sind in § 13 Abs. 1 TMG geregelt.

> *„Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten [...] in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung und Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn des Verfahrens zu unterrichten.*"

Cookies stellen ein automatisiertes Verfahren im Sinne des § 13 Abs. 1 Satz 2 TMG dar. Damit enthält das bestehende Recht bereits die Verpflichtung, vor dem Einsatz von Cookies – wie von der E-Privacy-Richtlinie gefordert – zu informieren. Neben der Beachtung dieser Informationspflicht kommt es für eine rechtmäßige Datenverarbeitung darauf an, ob hier eine gesetzliche Erlaubnis oder eine Einwilligung des Nutzers vorliegt. Ein allgemeines Einwilligungserfordernis regelt § 12 Abs. 1 TMG. Dort heißt es wie folgt.

> *„Der Diensteanbieter darf personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.*"

Ohne Einwilligung dürfen personenbezogene Daten im Zusammenhang mit der Bereitstellung von Telemedien also nur verarbeitet werden, wenn der Gesetzgeber dies ausdrücklich erlaubt. Eine solche gesetzliche Erlaubnis enthält § 15 Abs. 1 Satz 1 TMG für die sog. Nutzungsdaten; § 15 Abs. 1 Satz 1 TMG lautet wie folgt.

> *„Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten).*"

Nutzungsdaten sind Daten, die während der Nutzung eines Telemediums anfallen. Ohne Einwilligung dürfen solche Nutzungsdaten nur erhoben und verarbeitet werden, wenn dies für die Inanspruchnahme des Telemediums erforderlich ist. Als Nutzungsdaten kommen dabei u.a. in Cookies gespeicherte Daten in Frage. Damit dürfen Daten ohne die Einwilligung des Nutzers in Cookies erhoben und gespeichert werden, wenn dies aus technischen Gründen für die Inanspruchnahme des Telemediums erforderlich ist.

Zur Form der Einwilligung bestimmt § 13 Abs. 2 TMG, dass diese elektronisch (basiert) erklärt werden kann. Nach § 13 Abs. 2 TMG ist eine elektronisch erklärte Einwilligung nur dann wirksam, wenn die folgenden Voraussetzungen kumulativ erfüllt sind:

- die Einwilligung muss bewusst und eindeutig erteilt werden
- die Einwilligung muss protokolliert werden
- der Nutzer muss den Inhalt der Einwilligung jederzeit abrufen können und
- der Nutzer muss die Einwilligung mit Wirkung für die Zukunft jederzeit widerrufen können.

Gemäß § 13 Abs. 3 TMG muss der Nutzer zudem vor Erklärung der Einwilligung auf das Widerrufsrecht hingewiesen werden. Dieser Hinweis muss für den Nutzer jederzeit abrufbar sein.

§ 12 Abs. 1 TMG sowie § 15 Abs. 1 Satz 1 TMG und damit das strenge Einwilligungserfordernis gelten nur für personenbezogene Daten. Cookies haben jedoch nicht per se einen Personenbezug, denn nicht jedes Cookie speichert personenbezogene Daten bzw. macht eine Identifizierung des konkreten Nutzers möglich. Dies hängt stets von den Umständen des Einzelfalls und Art der mit einem Cookie gespeicherten und ausgelesenen Daten ab. Das gesetzlich geregelte Einwilligungserfordernis erfasst daher einzelne Anwendungsbereiche von Cookies, nämlich konkret den Fall, dass das eingesetzte Cookie personenbezogene Daten beinhaltet sowie den Fall, dass die mit dem Cookie erhobenen Daten mit anderweitig erhoben personenbezogenen Daten des Nutzers verknüpft werden.

Nach § 15 Abs. 3 TMG dürfen ohne Einwilligung Nutzungsprofile, insbesondere zu Werbezwecken, wie dies etwa im Rahmen nutzungsbasierter Online-Werbung häufig geschieht, bei Verwendung von Pseudonymen erstellt werden, sofern der Nutzer dem nicht widersprochen hat und der Nutzer auf dieses Widerspruchsrecht hingewiesen wurde. § 15 Abs. 3 TMG lautet wie folgt.

> *„Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden."*

Damit sieht § 15 Abs. 3 TMG als Ausnahme vom generellen Einwilligungserfordernis ausdrücklich ein Opt-out-Verfahren (Opting-out = das Nicht-Mitmachen) für die Erstellung pseudonymer Nutzungsprofile zu Werbezwecken vor. Sofern also Cookies dem pseudonymen Tracking zu Werbezwecken dienen, wie dies typischerweise der Fall ist, genügt nach den bestehenden gesetzlichen Bestimmungen das in § 15 Abs. 3 TMG geregelte Opt-out-Verfahren. Das geltende Recht ist hier eindeutig.

3.3.2. Die Cookie-Richtlinie

Die in Cookies abgelegten Daten geben Aufschluss über Art und Umfang der Nutzung von Online-Angeboten. Es handelt sich bei diesen Daten daher zunächst grundsätzlich um Nutzungsdaten im Sinne des deutschen Telemediengesetzes (TMG).

Nach dem Wunsch des EU-Parlaments sollte eine neue Richtlinie die Schaffung von mehr Transparenz und Sicherheit für die Verbraucher ermöglichen. Von besonderem Interesse für die digitale Wirtschaft waren die zur sogenannten E-Privacy-Richtlinie vorgesehenen Änderungen. Konkret geht es um die neu eingefügten Datenschutz-Vorgaben hinsichtlich der Voraussetzungen für die Nutzung von auf dem Endgerät eines Nutzers gespeicherten Informationen (auch Cookie-Richtlinie). Im Zuge der Neuregelung wurde insbesondere Art. 5 Abs. 3 der E-Privacy-Richtlinie wie folgt neu gefasst.

„(3) Die Mitgliedstaaten *stellen sicher, dass die* ***Speicherung*** *von Informationen oder der* ***Zugriff*** *auf* ***Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind****, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von* ***klaren und umfassenden Informationen****, die er gemäß der Richtlinie 95/46/EG u.a. über die Zwecke der Verarbeitung erhält, seine* ***Einwilligung*** *gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann."*

Die in diesem Artikel der E-Privacy-Richtlinie angesprochenen Informationen können dabei in vielfältiger Weise gespeichert und ausgelesen werden. Cookies stellen dabei zwar nur eine mögliche, jedoch die wohl bekannteste Art der Verarbeitungsmöglichkeit dar. Vor allem deshalb hatte sich schnell der Begriff „Cookie-Richtlinie" eingebürgert.

Die Richtlinie fordert eine strikte Einwilligung des Nutzers zu den dort benannten Handlungen – also zum Beispiel für das Setzen und Auslesen von Cookies auf dem Computer des Nutzers. Bei den verarbeiteten Informationen muss es sich nicht ausschließlich um personenbezogene Daten im Sinne der Richtlinie 95/46/EG handeln. Ausgenommen sollen – wie dargestellt – nur solche technischen Speicherungen sein, die für die Diensterbringung erforderlich oder vom Nutzer ausdrücklich erwünscht sind.

Gemäß Art. 2h) der angesprochenen Richtlinie 95/46/EG ist eine Einwilligung der betroffenen Person erforderlich, denn *„jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden".*

Vor der Einwilligung soll der Nutzer umfassend informiert werden. Nutzern sollen klare und verständliche Informationen bereitgestellt werden, wenn sie irgendeine Tätigkeit ausführen, die zu einer Speicherung oder einem Zugriff auf entsprechende Informationen führen könnte. Hier soll die Benutzerfreundlichkeit im Vordergrund stehen. Ausnahmen sollen nur dort erlaubt sein, wo die technische Speicherung oder der Zugriff unverzichtbar sind, um die Nutzung eines vom Teilnehmer oder Nutzer ausdrücklich angeforderten Dienstes zu ermöglichen. Die insoweit aufgestellten Vorgaben sind hinreichend deutlich. Genauere Vorgaben, wie eine solche Einwilligung erklärt werden kann, macht die Richtlinie jedoch nicht.

Der Arbeitskreis der europäischen Datenschutzbeauftragten (sog. Art. 29 Datenschutzgruppe) hat hervorgehoben, dass die von der Richtlinie geforderte Einwilligung stets einer aktiven Handlung bedarf, um wirksam zu sein. Eine nachträgliche Genehmigung sei dafür nicht ausreichend. Nachfolgende Möglichkeiten kämen nach Ansicht der Gruppe hier in Frage:

- Einwilligung über eine vorgeschaltete Startseite (splash screen), auf welcher der Nutzer über die verwendeten Cookies aufgeklärt wird und seine Einwilligung abgeben kann
- Einwilligungsmöglichkeit über ein statisches Banner („static information banner") am Kopf der Website, das Banner verlinkt dabei auf die Datenschutzerklärung
- Social-Plug-ins werden vor Aktivierung der Funktion zunächst standardmäßig inaktiv ausgeliefert (vgl. „2-Klick-Lösung" bei heise online)

Dies bedeutet jedoch nicht, dass die Nutzer eine Einwilligung nicht auch anders als durch das Ankreuzen einer entsprechenden Option (Opt-in) erklären könnten. Aus den Erwägungsgründen des Richtlinienentwurfs geht nämlich auch hervor, dass die Einwilligung des Nutzers ausdrücklich zusätzlich über die Handhabung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung ausgedrückt werden kann, wenn es technisch durchführbar und wirksam ist. Nach Angaben des Berichterstatters des Europäischen Parlaments, Alexander Alvaro, soll eine solche Zustimmung zur Datenerhebung daher dann als erteilt gelten, wenn der Nutzer seinen Browser so eingestellt hat, dass dieser Cookies akzeptiert.

Lange war unklar, ob deutsche Telemedienanbieter nun auch die Vorgaben dieser Richtlinie umzusetzen haben. Im Februar 2014 bestätigte die EU-Kommission auf Anfrage durch den BVDW allerdings, dass die derzeitigen Regelungen im deutschen Telemediengesetz (TMG) den Datenschutzstandards der „Cookie-Richtlinie" entsprechen.

Obwohl die Bundesregierung, bestätigt durch die EU-Kommission, der Ansicht ist, dass die Regelungen der Cookie-Richtlinie im TMG bereits umgesetzt sind, lässt sich zunächst ein Widerspruch nicht von der Hand weisen. Während die Cookie-Richtlinie eine Einwilligung fordert, lässt § 15 Abs. 3 TMG eine Widerspruchslösung genügen. § 15 Abs. 3 TMG und die Cookie-Richtlinie stehen jedoch nicht zwingend im Widerspruch zueinander. Nach Erwägungsgrund 66 der E-Privacy-Richtlinie können für die Einwilligung in den Gebrauch von Cookies erleichterte Anforderungen gelten.

Auch der Art. 29 Datenschutzgruppe (s. dazu bereits oben unter II.A.2), der für eine wirksame Einwilligung eine aktive Handlung des Nutzers fordert, geht davon aus, dass der Nutzer eine Einwilligung wirksam auch anders als durch das Ankreuzen einer Option bzw. Checkbox, also anders als durch ein reines Opt-in, erklären kann. So ist beispielsweise denkbar, dass der Nutzer durch den Verbleib auf der Website sowie das Weitersurfen und den nicht getätigten Widerspruch konkludent eine Einwilligung erteilt. Es kommt also vielmehr auf die Klarheit und Eindeutigkeit der Information bzw. des Hinweises an.

Für deutsche Website-Betreiber gelten daher die im TMG enthaltenen Regelungen. Daran wird auch die neu aufgewärmte Diskussion um eine Umsetzung der E-Privacy-Richtlinie in Deutschland nichts ändern. Diese ist nicht nur politisch motiviert, sie kommt auch noch zur Unzeit. Denn die Kommission fängt bereits diesen Sommer mit der Evaluierung der bereits

bestehenden Richtlinie an – mit dem Ziel, diese zu überarbeiten. Insofern sollte sich die Bundesregierung eher darauf konzentrieren, als vermeintlich bereits geklärte Fragen wieder „aufzuwärmen".

3.3.3. Fazit

Ein aktives Einwilligungserfordernis ist damit für den Einsatz von Cookies nicht gegeben. Allerdings muss auf die Verarbeitung von Nutzungsdaten in Cookies und auf das diesbezügliche Widerspruchsrecht des Nutzers deutlich – durch Informationen in einer leicht erkennbaren und zugänglichen Datenschutzerklärung – hingewiesen werden. Nutzungsprofile dürfen nur pseudonym angelegt werden und eine weitere Erhebung und Nutzung muss nach Widerspruch durch den Nutzer unterbleiben. Gesetzlich zwar nicht erforderlich, aber oft zu beobachten und unterstützend möglich, ist der Einsatz von Hinweisbannern, die bei Aufruf der Website oder dem Start einer App auf den Zugriff von im Gerät/Browser gespeicherten Informationen informieren.

Für nutzerbasierte Online-Werbung (OBA) existieren bereits selbstregulierende Strukturen der digitalen Wirtschaft. Seit 2012 können Endnutzer im Rahmen der seitens des BVDW maßgeblich vorangetriebenen Selbstregulierungsinitiative von Deutscher Datenschutzrat Online-Werbung (DDOW) durch ein deutlich sichtbares Datenschutzicon, ihre eigene Kontrolle über die Cookie-Nutzung walten lassen. Mehr dazu lesen Sie in Abschnitt „5. Selbstregulierung in Deutschland (DDOW)".

Darüber hinaus hat Google im Juli 2015 einen eigenen Vorstoß zur Implementierung solcher Hinweise auf eine Cookie-Nutzung sowohl auf Websites als auch bei Apps gemacht. Nach der Google Richtlinie zur Einwilligung der Nutzer[4] in der EU müssen u.a. Teilnehmer der Google-Programme AdSense, DoubleClick und DoubleClick Ad Exchange, Hinweise auf eine Cookie-Nutzung und die Erfassung und Übertragung von Daten implementieren. Auch die IAB Europe verfolgt einen vergleichbaren Ansatz und sieht in einer Vorgabe an ihre Mitglieder[5] ebenfalls die Implementierung von Hinweisen entsprechend vor.

4. Alternative Tracking-Technologien

Bei den Tracking-Technologien, die als ergänzende Alternative oder kompletter Ersatz bei Cookies zum Einsatz kommen, unterscheidet man prinzipiell zwischen Verfahren, die in Webbrowsern zum Einsatz kommen und Lösungen, die auf die speziellen technischen Gegebenheiten in mobilen Apps zugschnitten sind.

4.1. Browser-basierte Technologien

Die verschiedenen Methoden zur Re-Identifikation eines Webclients, die im Laufe der Zeit vom Markt entwickelt und in den folgenden Abschnitten vorgestellt werden, benutzen sehr unterschiedliche technische Herangehensweisen. Die Verfahren unterscheiden sich auch erheblich in den Kriterien Genauigkeit und Reichweitenrelevanz, zwei Faktoren, die am Ende maßgeblich mit über ihre praktische Nutzbarkeit für den gewünschten Zweck entscheiden.

[4] http://www.google.com/about/company/user-consent-policy.html
[5] http://www.iabeurope.eu/policy/e-privacy/five-practical-steps-comply-eu-eprivacy-directive

4.1.1. Fingerprinting

Als Fingerprinting werden im Kontext von IT-Systemen Verfahren bezeichnet, deren Ziel es ist, ein Gerät anhand einer Kombination von Hard- und Software-Merkmalen wiederzuerkennen. Kann man viele solcher Merkmale ermitteln, ergibt sich zwangsläufig eine riesige Menge möglicher Kombinationen. Die Wahrscheinlichkeit, dass ein zweites Gerät exakt dieselbe Kombination von Merkmalen aufweist, ist dann sehr gering und die Merkmalskombination wird zu einem (nahezu) eindeutigen Schlüssel. Man unterscheidet zwei Arten von Fingerprinting: Browser- und Canvas-Fingerprinting.

Browser-Fingerprinting

Beim Browser-Fingerprinting[6] wird diese Merkmalsliste von einem kleinen Programm in JavaScript zusammengetragen, das mit der Webseite ausgeliefert wird. Browser-Fingerprinting identifiziert damit, wie der Begriff schon sagt, den Browser – von dem es mehrere auf einem Gerät geben kann – und nicht das Gerät oder sogar den Nutzer. Die resultierende Liste von Merkmalswerten stellt dabei den „Fingerabdruck" eines Browsers dar und wird an eine Website zur Identifikation des Nutzers übertragen. Merkmale, die typischerweise dabei verwendet werden, sind unter anderem:

- Browser und dessen Version
- Betriebssystem und dessen Version
- Landes- und Spracheinstellungen
- Zeitzone
- Auflösung des Bildschirms
- Installierte Schriften
- Installierte Browser-Plug-ins.

Je nach Browser kann es darüber hinaus noch eine Vielzahl weiterer Merkmale geben, die für diesen Zweck genutzt werden können, unter anderem:

- Log-in-Status für Facebook, Twitter, Amazon etc.
- Dauer für die Ausführung von JavaScript-Operationen
- Art und Weise, wie Texte pixelgenau auf dem Bildschirm dargestellt werden (siehe Canvas-Fingerprinting).

Die resultierende Merkmalsliste wird nach Fertigstellung meist einem zusätzlichen Hashing-Verfahren (Reduktion der Ziel(daten)menge) unterworfen. Dies geschieht, um relativ kurze Schlüssel gleicher Länge zu erzielen – üblich sind Schlüssellängen von 32 oder 64 Bit. Ohne Hashing wären diese Merkmalslisten unhandlich lang.

Obwohl ein 64 Bit langer Schlüssel eine Vielzahl von verschiedenen Werten aufweist, sind Fingerprints in der Praxis keine eindeutigen Erkennungsmerkmale. Die Wahrscheinlichkeit, dass zwei Systeme denselben Schlüssel bekommen, liegt in der Praxis zwischen 5 % und 20 %, weil es viele Ähnlichkeiten zwischen Browser-Installationen gibt.

[6] Eine gute Illustration für die Arbeitsweise dieser Technologie ist die Open-Source-Bibliothek *fingerprintjs*.

Bei mobilen Browsern ist die Einzigartigkeit und damit eindeutige Identifizierung eines Browsers noch geringer, da sich die Endgeräte eines bestimmten Modells mit derselben Version von Browser- und Betriebssystem sehr stark ähneln. Es gibt zum Beispiel keine individuellen Browser-Plug-ins, keine installierten Schriftarten, die Bildschirmgröße ist dieselbe etc.

Der zweite wichtige Nachteil des Fingerprintings – neben der Fehlerquote bei der Wiedererkennung – ist, dass sich die ermittelten Merkmale im Laufe der Zeit ändern können. Bei beispielsweiser Berücksichtigung der Browserversion beim Fingerprint ergibt sich nach Aktualisierung des Browser ein neuer Fingerprint. Alle Daten über dieses System, die mithilfe des alten Fingerprints abgelegt wurden, sind dann nicht mehr auffindbar und praktisch verloren.

Grundsätzlich gilt, je seltener Fingerprints sind, desto kürzer ist ihre Haltbarkeit. Bei kommerziellen Verfahren sind „Halbwertzeiten" von weniger als einem Monat nicht unüblich. Im Online-Advertising reicht dieser Zeitraum zwar meist aus, anders als ein Cookie kann mit dem Einsatz von Fingerprint aber nicht die bewusste Entscheidung des Nutzers gegen ein Tracking, dass durch Opt-out ermöglicht wird, festgehalten werden. Diese Willensäußerung würde, ebenso wie alle anderen Merkmale im Rahmen des Fingerprints, nach wenigen Wochen verloren gehen.

Fingerprinting ist ausschließlich zur (Wieder-) Erkennung eines Browsers nutzbar. Mit diesem Verfahren können keine weiteren Daten (z.B. über vergangenes Surf-Verhalten oder Interessen des Users) gespeichert werden. Die Speicherung solcher Daten passiert auf dem Webserver – mit dem Fingerprint als Schlüssel in einer Datenbank.

Browser-Fingerprinting basiert auf JavaScript. Deaktiviert der Nutzer JavaScript in seinem Browser, unterbindet er damit auch das Fingerprinting. Allerdings beeinträchtigt das ebenso die Nutzung vieler Websites. Regelmäßige Änderungen an der Browserkonfiguration führen zur Generierung neuer Fingerprints und invalidieren somit die bereits für diesen Browser serverseitig gespeicherten Daten. Eine zukünftige Datensammlung (mit dem jeweils neuen Fingerprint) kann so aber seitens des Nutzers nicht unterbunden werden. Browser-Plug-ins – zum Beispiel Adblock Plus, Ghostery oder DoNotTrackMe – können die Übermittlung des Fingerprints an den Webserver (auf dem die tatsächlichen Nutzungsdaten für diesen Nutzer gespeichert sind) unterbinden, indem das ausführende Skript vom Plug-in blockiert wird. Das Fingerprinting selbst wird dadurch zwar nicht verhindert, eignet sich jedoch auch nicht mehr zur eindeutigen Identifizierung eines Browsers.

Ein Löschen der gesammelten Informationen durch den Nutzer ist bei allen Fingerprinting-Verfahren ohne Mitwirkung des Verfahrensbetreibers nicht möglich, da die Informationen nicht auf der Client-Seite (also im Browser des Nutzers) abgelegt werden, sondern auf den Servern des Betreibers.

Canvas-Fingerprinting

Das Canvas-Fingerprinting ist eine Abwandlung des Browser-Fingerprintings. Grundlage dafür ist das HTML5-Canvas-Element, das erlaubt, mithilfe von JavaScript-Grafiken auf eine virtuelle Leinwand (engl.: canvas) zu zeichnen. Abhängig von verschiedenen Parametern weisen die so erstellten Grafiken subtile Unterschiede auf. Über JavaScript wird außerhalb des am Bildschirm

sichtbaren Bereichs ein Canvas-Element erzeugt. Darin werden in der Regel ein vorgegebener Text und eine farbige Grafik erzeugt. Über die auf dem Canvas verfügbare Funktion *toDataURL()* werden die Bildinformationen enkodiert. Aus den Pixeldaten wird über Hashing-Verfahren ein Schlüssel erstellt, der als Fingerprint dient.

Der Fingerprint kann vor allem zur Wiedererkennung von Hard- und Softwarekombinationen genutzt werden, jedoch nicht eigenständig zur eindeutigen Identifikation von Nutzern. Weiterhin können keine privaten Nutzerinformationen über das Fingerprinting ausgelesen und übermittelt werden. Über Kombination mit anderen Tracking-Alternativen kann jedoch eine ausreichend genaue Identifikation des Browsers erreicht werden.

Im mobilen Web führt, wie bereits im „Browser-Fingerprint" erläutert, die starke Standardisierung der Hard- und Softwarekomponenten dazu, dass die Mehrzahl der Prüfsummen keine Abweichung aufweist und daher das Fingerprinting keine genaue Unterscheidung vornehmen kann.

Zusätzlich zu den Einflussfaktoren des Browser-Fingerprintings haben folgende Kriterien Einfluss auf den Canvas-Fingerprint:

- Anti-Aliasing (Kantenglättung)
- Font-Smoothing (browser- und betriebssystemabhängige Schriftglättung)
- Grafikkarte und Treiberversion.

Für die Erstellung des Canvas-Fingerprints werden bevorzugt Zeichenketten benutzt, die alle Symbole des Alphabets inklusive Zahlen enthalten. In der nachfolgenden Grafik ist ein Canvas-Element zu sehen, auf dem diverse Zeichenketten sichtbar sind. Aus diesen Pixeldaten wird anschließend die Prüfsumme erstellt.

Abb.: Canvas-Element mit Ergebnis des Fingerprint-JavaScripts

Für das Canvas-Fingerprinting gelten als eine Unterkategorie des Browser-Fingerprintings, auch dessen beschriebenen Vermeidungsmöglichkeiten. Eine allgemeine Blockierung des Canvas-Elements ist aufgrund seiner breiten Nutzung bei der Darstellung von Web-Elementen nicht sinnvoll. Diskutiert wird bei den Browser-Anbietern eine Funktion, die beim Auslesen jedes Canvas-Elements den Nutzer um dessen Erlaubnis fragen würde. Dieses Vorgehen praktiziert

aktuell der nur wenig verbreitete Tor-Browser. Verhindert der Nutzer das Auslesen des Elements, werden im Hintergrund leere Pixelinhalte an den Empfänger übertragen.

4.1.2. Common-IDs

Voraussetzung für die Verwendung dieser Technologie ist die Nutzung von solchen Web-Angeboten, die Besuchern nur mit einer Registrierung und einem Log-in die Erreichbarkeit eines Angebotes ermöglichen. Diese Web-Angebote generieren für jeden Nutzer eine personenbezogene und eindeutige ID (Identifier), mit der alle Informationen über den Besucher gespeichert werden. Das Einverständnis zur Speicherung und Verarbeitung der personenbezogenen Daten erteilt der Nutzer dabei durch aktive Zustimmung, meist zum Beispiel durch Einwilligung der AGB bereits bei der Registrierung. Die Zugangsdaten großer Portale sind nicht nur zur Anmeldung auf dem Portal selbst gültig, sondern können auch auf anderen Websites zur Authentifizierung benutzt werden. Beispiele hierfür sind Facebook Connect, oder die IDs anderer großer Identitätsverwalter (Google, Microsoft, Yahoo), die sich an den OpenID-Standard halten.

Manche dieser Log-in-Portale stellen zusätzlich Schnittstellen bereit, mit denen auch Dritte (Third-Parties) auf die Identifier zugreifen können, sofern der Nutzer mit gleichem Browser bei dem entsprechenden Log-in-Portal angemeldet ist. Hiermit wird Website-Betreibern die Möglichkeit geschaffen, solche Features des Log-in-Portals in ihren Content zu integrieren, die über eine erleichterte Anmeldung hinausgehen. Ein bekanntes Beispiel dafür sind die Social-Plug-ins, die zum Beispiel Twitter, XING, Facebook oder Pinterest anbieten. Diese Schnittstellen liefern auf Anfrage in der Regel eine eindeutige Kennung des Portalnutzers zurück. Diese kann von der Third-Party genutzt werden, um selbst einen Pool an Unique Identifiern aufzubauen und in Form eines herkömmlichen Browser-Cookies diesen auf dem Endgerät des Nutzers zu hinterlegen. Bei erneutem Kontakt mit dem Log-in-Portal kann die ID neu abgefragt und das Nutzerprofil des Tracking-Dienstes wiederhergestellt werden, falls der Nutzer inzwischen seine Cookies gelöscht haben sollte. Da die ID des Log-in-Portals personenbezogen ist, können mit ihrer Hilfe Profile aufgebaut werden, die nicht nur über alle verfügbaren Browser auf einem Gerät, sondern auch über mehrere Endgeräte hinweg eine Identifikation des Nutzers erlauben.

Der Gebrauch von Common-IDs zur Profilbildung durch Dritte kann vom Nutzer unterbunden werden, indem er sich nach Nutzung eines Log-in-Portals stets abmeldet und seinen Browser während des Log-in-Status nicht zum Besuch anderer Web-Angebote nutzt.

4.1.3. eTag

Jede Kommunikation zwischen Webbrowser und Webserver läuft stets so ab, das der Browser eine Anfrage (engl.: „Request") an den Server schickt und dieser daraufhin eine Antwort (engl.: „Response") zurücksendet. Request und Response bestehen immer aus zwei Teilen: den eigentlich zu übertragenden Daten und einem Header[7] mit zusätzlichen Metadaten („Daten über die Daten").

Der eTag (Kurzform von entity tag) ist ein Feld im Header (sowohl von Request als auch bei Response) und wird für das Browsercaching genutzt. Dazu wird für jede vom Webserver angefragte Ressource (z.B. Grafik/en, Skript/e, Datei/en) eine Prüfsumme erstellt, abgelegt

[7] „Beim Hypertext Transfer Protocol (HTTP) werden über den Header HTTP-Cookies und Informationen wie Dateigröße, HTTP-Server- und User-Agent-Kennung und MIME-Typ übertragen.", https://de.wikipedia.org/wiki/Header

und als eTag mitgesendet. Wird die Ressource erneut angefordert, werden die Prüfsumme auf dem Webserver und die der Website miteinander verglichen, um festzustellen, ob sich die angefragte Ressource verändert hat. Wenn sich die Prüfsummen nicht voneinander unterscheiden, wird vom Browser die vorhandene Ressource aus dem Cache geladen.

Um ein Tracking über den eTag-Parameter durchführen zu können, muss auf den vom Webserver übermittelten Wert des eTag zugegriffen werden. Ein Weg dies zu erreichen, ist über JavaScript. Dieses kann jedoch nicht auf bereits gesendete Header-Informationen zugreifen. Hier wird über eine nachgelagerte Anfrage Abhilfe geschaffen, beispielsweise über einen Ajax-Call. Oft wird dafür eine Grafik mit 1x1 Pixel-Abmessung benutzt, die auf jeder Seite und auch Web-Unterseite integriert ist. Ist der Call erfolgreich, wird auch der eTag-Parameter im Header vom Webserver mitgesendet und kann vom JavaScript ausgelesen werden. Das Auslesen des eTag-Parameters kann ebenfalls auf Serverseite durchgeführt werden. Besitzt man den Wert des eTag, kann dieser ähnlich wie ein Cookie benutzt und mit profilbildenden Informationen angereichert, übertragen und abgespeichert werden.
Der eTag kann aus jeder geladenen Ressource auf einer Website eingesehen werden. In der Netzwerkübersicht aktueller Browser wird dieser angezeigt, wie im nachfolgenden Screenshot dargestellt.

Abb.: Server-Request-Header und dessen Response-Header inklusive eTag

Das Feld *If-None-Match* ist hierbei die clientseitige Prüfsumme, die mit der Prüfsumme auf dem Webserver verglichen wird. Hat sich die Ressource auf dem Webserver verändert, stimmen die Prüfsummen nicht mehr überein und wird vom Server entsprechend geladen.

Die Technologie, die für diese Art des Trackings benutzt wird, ist unabhängig von Cookies, JavaScript und IP-Adresse. Das bedeutet, dass das Tracking nicht durch Deaktivieren bzw. Löschen von Cookies oder den Einsatz von VPN-Verbindungen (Virtual Private Network) vermieden werden kann. Weiterhin gibt es keinerlei Opt-out-Möglichkeit für den Nutzer.

Um dennoch nicht getrackt werden zu können, müsste der Nutzer mit jedem Seitenaufruf seinen Browsercache löschen. Das permanente Löschen oder Deaktivieren des Browser-Caches kann jedoch zur Folge haben, dass der Nutzer erheblich in seinem Surfverhalten eingeschränkt wird. Ladezeiten werden erhöht, und für mobile Geräte bedeutet dies eine erhebliche Belastung des Datenvolumens. Selbst Browsereinstellungen, die bewirken, dass bei Beenden des Browsers der Cache gelöscht wird, bieten nur insofern einen Schutz, als dass der Nutzer nicht über mehrere Sessions hinweg getrackt werden kann. Innerhalb einer Session bleibt der Nutzer aber weiterhin trackbar.

4.1.4. Local Storage (auch Web Storage, DOM Storage)

Local Storage, manchmal auch Web Storage oder DOM Storage genannt, ist eine Möglichkeit, lokal solche Daten im Web-Browser zu speichern, die auch nach dem Schließen des Browser-Fensters oder dem Beenden des Programms weiterhin bestehen und jederzeit wieder ausgelesen werden können.

In der Vergangenheit war es in JavaScript unmöglich, Daten im lokalen Dateisystem des Endgerätes, auf dem der entsprechende Web-Browser läuft, zu lesen und/oder zu schreiben. Ein Zugriff auf die lokalen Dateien war unter anderem aus Gründen des Datenschutzes sowie zur Vermeidung von Virusinfektionen untersagt. Die einzige Methode, Daten abzulegen, die ein Schließen des Browserfensters bzw. ein Beenden des Browsers überleben, waren Cookies. Cookies sind aber, wie bereits beschrieben, hinsichtlich ihrer Größe stark beschränkt

Deshalb wurde mit HTML5 ein Verfahrensweg eingeführt, mit der sich Daten permanent speichern lassen, der aber zugleich so eingeschränkt ist, dass Vireninfektionen damit nicht praktikabel auszuschließen sind und ein Zugriff auf beliebige lokale Daten unmöglich ist. Web Storage wurde im Jahre 2013 seitens des World Wide Web Consortium (W3C) standardisiert[8]. Für die auf diese Art gespeicherten Daten gibt es keine formale Größenbeschränkung (Browser definieren allerdings individuell hohe Limits). Zudem können die Daten strukturiert werden: Der Programmierer hat die Möglichkeit, „Schlüsselnamen" zu definieren und jedem dieser Namen einen Daten-Wert zuzuweisen, der später wieder ausgelesen werden kann.

HTML5 Local Storage ist deshalb sehr flexibel und kann – ähnlich wie Cookies – sowohl direkt dazu verwendet werden, Daten über den Nutzer zu speichern, als auch den Nutzer wiedererkennbar zu machen, indem eine entsprechende ID im Local Storage abgelegt wird.

Die Verwendung von Local Storage ist nur mit JavaScript möglich. Deaktiviert der Nutzer JavaScript in seinem Browser, unterbindet er damit auch das Tracking. Allerdings beeinträchtigt das ebenso die Nutzung vieler Websites.

Moderne Browser bieten dem Nutzer vergleichbare Möglichkeiten zur Verwaltung von Local-Storage-Daten wie zur Verwaltung von Cookies: Man kann sich die Daten auflisten lassen und (gesamt oder gezielt) löschen. Der Apple Safari-Browser regelt die Zugriffsrechte, die ein JavaScript-Programm hat, dies nach vergleichbaren Regeln wie bei 3rd-Party-Cookies (s. o.). Das heißt, dass der Java-Script-Code in einer Website B nicht mehr auf Local-Storage-Daten zugreifen kann, die der Java-Script-Code auf einer Website A abgelegt hatte. Für künftige

[8] Siehe API for persistent data storage of key-value pair data in Web clients; *http://www.w3.org/TR/webstorage*

Versionen des Firefox-Browsers ist ein vergleichbares Verhalten in Diskussion. Softwareentwickler können deshalb nicht mehr generell davon ausgehen, die bestehenden Zugriffsbeschränkungen auf 3rd-Party-Cookies mithilfe von Local Storage umgehen zu können.

4.1.5. Flash-Cookies

Bei Flash-Cookies handelt es sich um Dateien, die von einer Website über den Adobe-Flashplayer auf einem Speicherort beim lokalen Endgerät browserübergreifend abgelegt, ausgelesen und verändert werden können. Angelegt werden dabei ebenfalls einzelne Textdateien pro Domain. Die Struktur und Ablagesystematik ähnelt also prinzipiell der des Browser-Cookiestore. Im Vergleich zu Browser-Cookies können Flashcookies mit 100 Kilobyte pro Domain aber deutlich mehr Daten speichern. Der ursprüngliche Einsatzzweck von Flashcookies ist, die Website in die Lage zu versetzen, im Interesse eines möglichst komfortablen Surferlebnisses sessionübergreifend Einstellungen für den Flashplayer zu verwalten.

Flashcookies werden aber in der Praxis häufig auch zum Tracking eingesetzt, indem die Website eine eindeutige ID oder Profilinformationen über den Flashplayer dort ablegt. Für diesen zweckgebundenen Einsatz von Flashcookies anstelle oder ergänzend zu Browser-Cookies gibt es mehrere Beweggründe:

- Flashcookies haben kein zeitliches Verfallsdatum
- bleiben beim Löschen der Browser-Cookies erhalten
- lassen sich über die Datenschutzeinstellungen im Browser nicht ablehnen und
- ermöglichen die Identifikation von Nutzern auf einem Endgerät über mehrere Browser hinweg.

Die praktische Bedeutung von Flash-Cookies nimmt allerdings zügig ab. Insbesondere wird Flash auf der Mehrzahl der neu verkauften Mobilgeräte und im Nachfolger des Browsers Internet Explorer sowie Microsoft Edge nicht mehr unterstützt. Auch der Browser Google Chrome wird Flashfilme in naher Zukunft nicht mehr in jedem Fall abspielen.

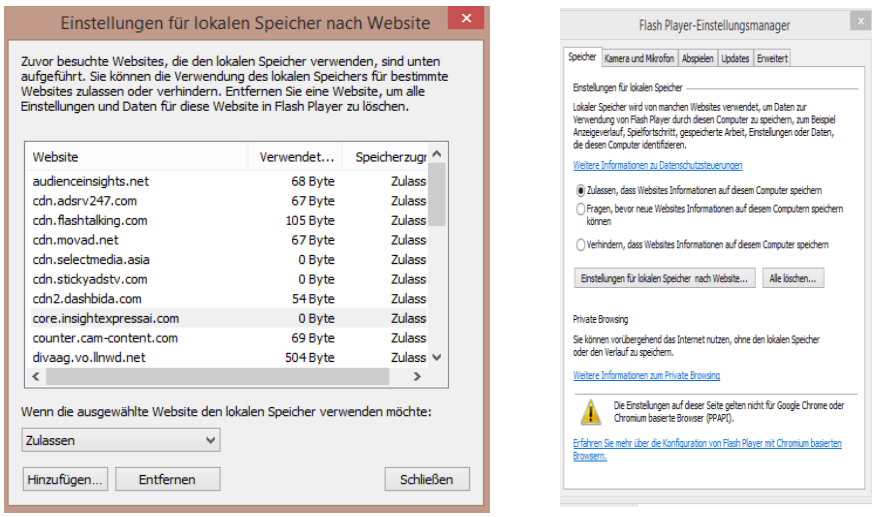

Abb.: Einstellungsmanager für Flash in Microsoft Windows 8

Flashcookies lassen sich bei den verbreiteten Betriebssystemen über den so genannten Flash-Player-Einstellungsmanager verwalten. Dieser ist über die Systemeinstellung des jeweiligen Endgeräts zugänglich. Im Einstellungsmanager kann das Setzen von Flashcookies über ein Sperrcookie unterbunden werden, von einer Einzelerlaubnis des Nutzers abhängig gemacht oder generell zugelassen werden. Letzteres obliegt der Voreinstellung des Managers.

Außerdem können vorhandene Flashcookies global oder selektiv gelöscht und Regeln zum Zulassen oder Sperren des Setzens von Flashcookies für einzelne Domains verwaltet werden. Wie bereits erwähnt bleiben Flashcookies auch beim Löschen der Browser-Cookies erhalten, zudem werden beim Löschen aller temporären Internetdateien nicht bei allen Browsern die Flashcookies zuverlässig mitgelöscht. Generell vermeiden kann man Flashcookies nur durch ein über den Einstellungsmanager gesetztes Sperrcookie oder durch Verzicht auf die Nutzung des Flashplayer-Plug-ins.

4.1.6. Authentication Cache

Die Nutzung des Authentication Cache ist eine Möglichkeit, sich für das Tracking die Tatsache zunutze zu machen, dass Web-Browser die erforderlichen Zutrittsdaten (Name und Passwort) für den Zugriff auf eine passwortgeschützte Website cachen (für die Wiederverwendung speichern).

Tracking über den Authentication Cache basiert auf der sogenannten „HTTP basic authentication". Dabei wird serverseitig festgelegt, dass für den Zugriff auf eine Ressource bei diesem Webserver im Header des entsprechenden HTTP-Requests eine dem Server bekannte Kombination von Namen und Passwort übergeben werden muss. Ist das nicht der Fall, liefert der Server nicht diese Ressource bzw. Seite zurück, sondern den Fehlerstatus „HTTP 401 Not Authorized" bzw. „HTTP-Fehler 401 Unauthorized". Bekommt ein Webbrowser diesen Fehlercode (Fehleranzeige) beim Aufruf einer Seite vom Server zurück, zeigt er automatisch ein kleines Dialogfenster, in dem der Nutzer Name und Passwort eingeben kann. Damit wird dann ein zweites Mal versucht, diese Seite anzufordern. Das ist ein Standardverhalten, dass in allen Browsern „fest eingebaut" ist.

Damit der Nutzer nicht für jede Seite auf einem Webserver, die auf diese Art zugangsgeschützt ist, Name und Passwort immer erneut eingeben muss, erfolgt bei allen Browsern eine Zwischenspeicherung dieser Angaben. Insbesondere bei einem zweiten Aufruf derselben Seite oder bei einem Link auf einer anderen Seite desselben Servers werden der gespeicherte Nutzername und das Passwort automatisch mitgegeben.

Möchte man diesen Mechanismus zum Tracking verwenden, geht man dabei in der Regel wie folgt vor.

1. Auf einer Website wird ein Aufruf (Request) einer bestimmten Ressource (zum Beispiel eines Pixels) auf dem Server durch ein Stück JavaScript-Code integriert. Diese Ressource ist, wie oben beschrieben, zugangsgeschützt.
2. Beim ersten Aufruf dieser Ressource, ist kein Name/Passwort bekannt. Also wird auch keine dieser Daten an den Server mitübergeben. In diesem Fall liefert der Server nicht nur den Fehlercode 401 zurück, sondern zugleich eine zulässige Kombination von

Name+Passwort. Dabei handelt es sich aber nicht um eine Kombination von Name+Passwort, sondern in Wirklichkeit um eine neue Nutzer-ID.

3. Ein Stück JavaScript-Code in der Seite nimmt die vom Server gelieferte Kombination von Name+Passwort entgegen und ruft die Ressource einfach gleich noch einmal auf – diesmal aber mit Name+Passwort im HTTP-Header. Der Server liefert die Ressource dann zurück – und legt diese Kombination von Name+Passwort in seinem Authentification Cache ab.
4. Bei allen folgenden Aufrufen der Ressource ergänzt der Browser nun automatisch Name+Passwort beim Request. Dadurch meldet sich der Browser quasi bei jedem Request mit einer eindeutigen ID (Name+Passwort) beim Server an.

Theoretisch können durch die geeignete Auswahl einer (langen) Datenkombination von Name+Passwort auf diese Weise nicht nur eine ID gespeichert, sondern auch Nutzerdaten abgelegt werden. In der Praxis ist es aber meist sinnvoller, sich auf eine ID zu beschränken, bei der es sich um den Schlüssel für einen Nutzer-Datensatz auf dem Server handelt. Auf diese Weise entfallen mögliche Größenbeschränkungen.

Authentication Tracking ist keine universelle Tracking-Methodik. Wie praktikabel dieser Ansatz ist, hängt davon ab, wie lange der jeweilige Browser Name+Passwort im Cache behält. Einige Browser tun dies nur für die Dauer einer Session (solange ein Browserfenster geöffnet ist) oder sogar noch kürzer. Dann ist dieser Verfahrensweg untauglich. Gerade Safari von Apple kann aber dazu gebracht werden, den Cache lange zu erhalten. So lässt sich dann die Default-Einstellung von Safari, 3rd-Party-Cookies nicht zuzulassen, mit dieser Technik plus etwas Aufwand umgehen.

Das Tracking über den Authentication Cache basiert auf JavaScript. Deaktiviert der Nutzer JavaScript in seinem Browser, unterbindet er damit auch das Tracking. Allerdings beeinträchtigt das ebenso die Nutzung vieler Websites. Adblocker können zudem den Zugriff auf die Domain des Webservers, auf dem die angesprochene Ressource liegt, unterbinden. Das ist immer dann möglich, wenn diese Ressource nicht in derselben Domain liegt, wie die Websites, auf denen das Tracking benötigt wird – die vorherrschende Konstellation im Online-Advertising.

4.2. Mobile app-basierte Technologien

Das Setzen von Cookies innerhalb von Apps ist zwar – mittels eines HTML-View – generell möglich, unterliegt aber einigen Beschränkungen, welche die Nutzung für das Tracking erheblich einschränken. Diese Einschränkung ergibt sich daraus, dass die so gesetzten Cookies nur in der App auslesbar sind, in der das Cookie gesetzt wurde und entsprechend gewonnene Informationen nicht in anderen Apps nutzbar sind. Durch diese Beschränkung ist der Einsatz von Cookies für die gezielte Aussteuerung von Werbung in der Praxis sehr stark eingeschränkt.

Als Alternative werden für das Tracking innerhalb von Apps die sogenannten Advertising-IDs verwendet. Solche IDs sind sowohl auf Android-basierten Geräten als auch für iOS-basierte Geräte verfügbar. Weiterhin sind diese IDs für das jeweilige Endgerät eindeutig. Es ist daher möglich, Informationen die in einer bestimmten App anhand einer solchen ID erfasst wurden, auch in einer anderen App – auf demselben Endgerät – zu verwenden.

Die hier beschriebenen IDs lassen sich sowohl beim mobilen Betriebssystem iOS als auch bei Android jederzeit durch den Nutzer zurücksetzen. Dies hat zur Folge, dass über das Endgerät gesammelte Informationen diesem nicht weiter zugeordnet werden können. Alle Informationen, die vor dem Zurücksetzen gesammelt wurden, sind dann nicht mehr nutzbar – ein Effekt, der dem Löschen eines Cookies gleichkommt. Weiterhin ist es dem Nutzer möglich, sich beim Einsatz von IDs generell abzumelden (Opt-out). Jeder Tracking-Anbieter muss daher zunächst prüfen, ob der User einen entsprechenden Opt-out gesetzt hat, bevor Daten anhand der IDs für Targeting-Maßnahmen erfasst werden. Die Möglichkeit des Zurücksetzens und des Opt-out (Abmelden) für werbliche Zwecke steht dem Nutzer bei beiden Herstellern im Menü des jeweiligen Endgeräts zur Verfügung. Eine Schritt-für-Schritt-Anleitung ist auf den Websites beider Hersteller vorhanden.

4.2.1. Device abhängige IDs von Apple iOS

Bei iOS konnte bis Version 5 des Betriebssystems der sogenannte Unique Device Identifier (UDID) für das Tracking verwendet werden. Der UUID (Universally Unique Identifier) brachte aber große Datenschutzprobleme mit sich, da er für ein Gerät eindeutig und ewig gültig ist. Damit waren anbieterübergreifende Verhaltensprofile möglich, gegen deren Erstellung sich der Nutzer nicht wehren konnte. Apple hat den UUID deshalb ab September 2012 mit Version 6 von iOS durch die sogenannte ID for Advertisers (IDFA) ersetzt und deren Verwendung unter den Vorbehalt des Nutzerwiderspruchs gestellt. Die Verwendung der alten UDID ist seitdem untersagt.

Die Verwendung der IDFA funktioniert wie folgt. Zunächst wird mittels der Methode „advertisingTrackingEnabled" geprüft, ob der Nutzer zur Verwendung der ID bei Targetingzwecken widersprochen hat. Ist dies nicht der Fall, wird die IDFA mittels Verfahren „Advertising Identifier" ermittelt und kann für die Erhebung von Informationen verwendet werden.

4.2.2. Device abhängige IDs von Google Android

Bei Android ist die Situation vergleichbar: Zunächst stand zur Identifikation eines Geräts lediglich die Android-ID zur Verfügung. Auch diese ist wie die UDID permanent und ihre Verwendung vom Nutzer nicht kontrollierbar. Seit Oktober 2013 steht auf Endgeräten, welche die „Google Play Services" der Version 4.0 oder höher verwenden (typischerweise Android-Version 2.3 oder höher), die Google-Advertising-ID zur Verfügung. Seit August 2014 ist die Verwendung der Google-Advertising-ID anstelle der Android-ID für alle Apps im Google Play Store zwingend vorgeschrieben.

Die Google Advertising-ID kann von jeder App benutzt werden, indem von Google Play Services bereitgestellte Funktionen verwendet werden. Hierbei muss mittels der Methode „isLimitAdTrackingEnabled()" zunächst geprüft werden, ob der Nutzer zur Verwendung der Advertising ID widersprochen hat. Sollte dies nicht der Fall sein, wird mit der Methode „getId()" die dem Endgerät zugeordnete eindeutige Advertising-ID ermittelt. Die Google-Advertising-ID ist eine alphanumerische Zeichenkette die (realtypisch) so aussieht: „38400000-8cf0-11bd-b23e-10b96e40000d". Der Tracking-Anbieter ist nun in der Lage, Informationen, die er über den Nutzer sammeln möchte, anhand dieser ID pseudonymisiert abzuspeichern und den Nutzer später mittels der ID auch in anderen Apps wiederzuerkennen.

4.3. Datenschutzrechtliche Aspekte bei alternativen Tracking-Technologien

Die hier vorgestellten Methoden unterscheiden sich von „klassischen" Cookies teilweise nur in technischer Hinsicht. Mit Blick auf DOM Storage oder Flash-Cookies bleibt es daher bei den aufgezeigten Grundsätzen. Werden in diesem Rahmen Nutzungsdaten erhoben, können diese nach § 15 Abs. 3 TMG für die Zwecke der Werbung und Marktforschung in pseudonym angelegten Nutzerprofilen verarbeitet werden. Auch hier muss der Nutzer in einer Datenschutzerklärung auf diesen Umstand hingewiesen und ihm die Möglichkeit gegeben werden, dieser Nutzung zu widersprechen („Opt-out").

Dieses Regime gilt auch für die app-basierten Technologien. Die Möglichkeit, Nutzerprofile über Apps hinweg mittels einer zuvor vergebenen ID wiederzuerkennen, betrifft allein das vergebene Pseudonym.

Andere, hier vorgestellte Technologien, wie eTag basieren zwar auf dem Surfverhalten (Page Impressions bzw. Website-Aufrufe), beinhalten jedoch keinerlei individuelle Informationen, mit denen ein Personenbezug hergestellt werden kann. Das Vergleichen von Prüfsummen ist ein rein technischer Vorgang und erfolgt damit in anonymer Weise, ohne den Bezug zum Nutzer. Für solche alternative Tracking-Technologien, die auf anonyme Daten zurückgreifen, gilt daher nichts anderes als für jene zur Verarbeitung anonymisierter Daten. Auch sie sind von der Anwendung der Datenschutzgesetze befreit, wenn sie nur auf anonyme Daten zurückgreifen.

5. Selbstregulierung in Deutschland (DDOW)

Begleitend zu den datenschutzrechtlichen Entwicklungen hat sich eine effektive europäische Selbstregulierung im Bereich nutzerbasierte Online-Werbung herausgebildet. Der Deutsche Datenschutzrat Online-Werbung (DDOW) ist die freiwillige Selbstkontrolleinrichtung (Selbstregulierung) der digitalen Werbewirtschaft für nutzungsbasierte Online-Werbung in Deutschland. Bei der nutzungsbasierten Online-Werbung (Online Behavioral Advertising, kurz: OBA) werden endgerätebezogene Daten zur Webnutzung in anonymisierter oder pseudonymisierter Form erfasst und zur zielgruppenspezifischen Auslieferung von Online-Werbung verwendet.

Der DDOW hat Kodizes entwickelt, die Verbrauchern über den gesetzlichen Rahmen hinaus Transparenz, verständliche Informationen und einen einfach handhabbaren Entscheidungsmechanismus zur Kontrolle von nutzerbasierter Online-Werbung bereitstellen. Die gesetzlichen Datenschutzbestimmungen in Deutschland werden durch die Vorgaben der Kodizes ergänzt.

OBA im Sinne des definierten Kodexes ist die Erhebung und Verarbeitung von Daten, die während des Besuchs einer oder mehrerer Websites über einen bestimmten Zeitraum anfallen, mit dem Ziel, anhand der erfassten Daten Interessenpräferenzen von Verbrauchern festzustellen, um Werbung auszuliefern, die deren Vorlieben und Interessen entsprechen könnte. Dabei ist es unerheblich, ob bei OBA personenbezogene Daten erhoben und verarbeitet werden. Sämtliche Vorgaben gelten auch dann, wenn mit nicht-personenbezogenen Daten gearbeitet wird.

Unter OBA fällt keine rein kontextabhängige Werbung, wie zum Beispiel bei suchbegriffsbasierter Werbung in Suchmaschinen oder bei der auf bestimmten Schlüsselbegriffen fußenden des Website-Inhalts. Unter OBA fällt genauso wenig die direkte Abfrage von Interessen beim Verbraucher (z.B. fakultative Informationen), die aus einem Registrierungsprozess für Online-Dienste resultiert.

5.1. Technologieneutraler Geltungsbereich

Die OBA-Selbstregulierung gilt grundsätzlich für alle Tracking-Methoden, die eingesetzt werden, unabhängig davon, ob HTML-Cookies oder andere Tracking-Verfahren verwendet werden. Alle Pflichten nach dem OBA Framework müssen grundsätzlich bei allen genutzten Tracking-Verfahren eingehalten werden. Die OBA-Selbstverpflichtung ist für alle Display-Werbeformen einzuhalten. Für den Bereich Mobile (Mobile-Browser, In-App-Werbung) soll die OBA-Selbstverpflichtung demnächst, d. h. voraussichtlich 2015/2016, auch gelten. Für den Bereich der Video-Werbung gilt die Verpflichtung bisher nicht, da es hier noch keine technische Umsetzung gibt.

5.2. Die Informationspflichten

Für alle Unternehmen, die OBA betreiben, gilt, dass auf den eigenen Websites klar und verständlich auf die Datenerhebung und -verarbeitung für OBA-Zwecke hingewiesen werden muss. Die geforderten Angaben beziehen sich auf

- die Identität und Kontaktdaten des Telemedienanbieters
- die Art der Daten, die für OBA-Zwecke erfasst und verarbeitet werden, einschließlich eine Angabe darüber, ob diese Daten oder Teile dieser Daten gem. § 3 Bundesdatenschutzgesetz "personenbezogene Daten" sind
- den Zweck, für den OBA-Daten verarbeitet werden einschließlich Information; hier ist wichtig, ob und wem solche Daten übermittelt werden können (Datenübermittlung an Dritte)
- den Hinweis, dass sich der Telemedienanbieter dem Kodex unterworfen hat und einen Link zu den Seiten des DDOW bereithält.

Die Kennzeichnungspflicht der OBA-Dienstleister (Drittparteien) beinhaltet Nachfolgendes:
Generell muss im Bereich nutzungsbasierter Online-Werbung in „zwei Welten" gedacht werden. Die Datenerhebung und -verwendung für Werbezwecke kann durch einen Website-Betreiber bzw. Telemedienanbieter – sogenannte Erstpartei – ausschließlich auf der Website erfolgen, die der Verbraucher besucht. Bezugspunkt für die Selbstregulierung ist hier die Website, auf der der Datenumgang stattfindet.

Nutzungsbasierte Werbung kann aber auch durch einen OBA-Dienstleister – sogenannte Drittpartei – erfolgen. Hier erhebt und nutzt nicht der Telemedienanbieter bzw. die Website, die der Verbraucher besucht, die Daten. Dies geschieht vielmehr domainübergreifend durch den Dritten, den OBA-Dienstleister. Drittparteien sind unter anderem Werbenetzwerke oder Online-Mediaagenturen. In diesen Fällen ist das Werbemittel, z.B. die Display-Anzeige, der Bezugspunkt für die Selbstregulierung.

Zusätzlich zu den oben beschriebenen Informationen weisen OBA-Dienstleister mittels eines einheitlichen Piktogramms im unmittelbaren räumlichen Zusammenhang mit dem jeweiligen Werbemittel auf den Einsatz von OBA hin. Diese Kennzeichnungspflicht gilt für alle Werbemittel, die entweder eine Datenerhebung starten oder auf der Basis bereits erhobener Daten ausgeliefert werden. Auf einen Blick sieht der Verbraucher, ob und welche OBA-Dienstleister Informationen für nutzungsbasierte Online-Werbung erheben und verwenden. Von dort aus kann über das zentrale Präferenzmanagement[9] Einsatz solcher Werbung direkt und einfach gesteuert werden. Damit schafft das Piktogramm Transparenz darüber, ob Nutzungsdaten für Werbezwecke verwendet werden und bildet die Grundlage einer informierten Entscheidung.

Abb.: OBA-Piktogramm

Die Kennzeichnungspflicht der Telemedienanbieter (Erstparteien) beinhaltet Nachfolgendes: Telemedienanbieter schaffen Transparenz auf ihren Websites mittels Verlinkung über einen eindeutigen Texthinweis (z.B. „nutzungsbasierte Online-Werbung") oder durch Verwendung des einheitlichen Piktogramms auf ihren Webseiten. Die Verlinkung muss auf jeder Website des Telemedienanbieters erfolgen, auf der nutzungsbasierte Werbung ausgeliefert wird oder Daten für nutzungsbasierte Werbung durch den Telemedienanbieter erhoben und verarbeitet werden.

5.3. Die Kontrollmöglichkeiten für Verbraucher

OBA-Dienstleister müssen einen Online-Mechanismus auf der eigenen Seite bereitstellen, der eine Entscheidung über die Erhebung und Verarbeitung von Daten für OBA-Zwecke ermöglicht. Dieser muss über das Piktogramm zugänglich sein. Zusätzlich sind alle OBA-Dienstleister verpflichtet, am anbieterübergreifenden Präferenzmanagement teilzunehmen. Dieses wird europaweit einheitlich bereitgestellt und ist unter anderem über meine-cookies.org erreichbar. Dort wird jeder einzelne OBA-Dienstleister gelistet. Damit besteht die Möglichkeit, über die Erhebung, Verarbeitung und Übermittlung durch OBA-Dienstleister einzeln oder gesamt mit nur einem „Klick" zu entscheiden.

Telemedienanbieter müssen es Verbrauchern ermöglichen, die Erhebung und Verarbeitung von Daten für OBA-Zwecke und die Übermittlung solcher Daten an Dritte auszuschließen. Telemedienanbieter stellen hierzu entweder einen entsprechenden Online-Mechanismus bereit oder der Website-Betreiber erläutert die endgerätebezogenen Einstellungsmöglichkeiten so, dass Verbraucher auf diese Weise ihre Präferenzen wahrnehmen können. Beides muss über die oben erwähnten Texthinweise oder über das Piktogramm zugänglich sein.

Mit den Kontrollmöglichkeiten für Verbraucher wird eine einfache und transparente Möglichkeit geschaffen, eine informierte Entscheidung in Bezug auf nutzungsbasierte Online-Werbung zu treffen.

[9] http://meine-cookies.org/cookies_verwalten/praeferenzmanager-beta.html

5.4. Weitere Verpflichtungen

Neben den oben beschriebenen Kernelementen besteht eine Reihe weiterer Verpflichtungen, nämlich wie folgt.

- Beim Einsatz spezieller Computerprogramme (bspw. Toolbars), die systematisch die aufgerufenen URLs erfassen, gilt eine explizite Einwilligungspflicht.
- Es ist unzulässig, im Rahmen von OBA Segmente zu bilden, die sich speziell an Personen unter 12 Jahren richten.

Unternehmen verpflichten sich zudem zu Aufklärungsmaßnahmen und zur Förderung der Medienkompetenz.

6. Ausblicke – Regelungen einer künftigen Datenschutzgrundverordnung

Die Möglichkeit, Nutzungsdaten pseudonymisiert verarbeiten zu können, ist essenziell für die digitale Wirtschaft. Die im deutschen Recht vorhandenen „Privacy-by-Design-Ansätze" wie die Pseudonymisierung müssen neben dem Instrument der Einwilligung bei der Verarbeitung von personenbezogenen Daten daher auch in die aktuell diskutierte EU-Datenschutzgrundverordnung aufgenommen werden. Ein striktes Einwilligungserfordernis ist nicht nur für den unkomplizierten Aufruf von Webangeboten impraktikabel, sondern es gewährt dem einzelnen Nutzer auch keinen wirksamen Rechtsschutz. Dass hier eher das Gegenteil der Fall ist, zeigen Angebote, die sich mithilfe einer allgemeinen Einwilligung eine wesentlich weitreichendere Nutzung der Daten vom User erlauben lassen, als dies allein zu Werbezwecken erforderlich wäre. Kaum ein Nutzer liest sich die teilweise umfangreichen Informationstexte durch, sondern klickt auf den Einwilligungsbutton, um möglichst schnell und unkompliziert das jeweilige Website-Angebot nutzen zu können.

Dies zeigt deutlich, dass dem Interesse der Nutzer am Schutz ihrer Daten am besten entsprochen wird, wenn sie ihre Klardaten gar nicht erst angeben müssen, und genau dies verhindert die pseudonyme Verarbeitung der Daten, wie das deutsche TMG sie ermöglicht. Es trägt dem Grundsatz der Datensparsamkeit Rechnung und ist „best practice", da „privacy by design" – denn die Daten sind für Dritte nicht rückbeziehbar. Gleichzeitig erlaubt diese Regelung die Werbefinanzierung der oft hochwertigen Webangebote durch die digitale Wirtschaft, an die wir uns alle gewöhnt haben und für die wir möglichst nichts zahlen wollen.

Experten

Der besondere Dank für die Entstehung dieser Publikation gilt den Autoren und den folgenden Unternehmen.

Prof. Dr. Christoph Bauer,
Geschäftsführer, ePrivacy GmbH

Markus Breuer,
Director Mobile & Emerging Channels, nugg.ad AG

Daniel Diebold,
Senior Dialog Infrastruktur Manager, United Internet Media AG

Dr. Frank Eickmeier,
Rechtsanwalt und Partner, UNVERZAGT VON HAVE Rechtsanwälte

Jörg Klekamp,
Vorstand, ADITION technologies AG,
Vorsitzender der Fokusgruppe Targeting im BVDW

Svenja-Ariane Maucher,
Rechtsanwältin und Counsel, King & Wood Mallesons LLP

Michael Neuber,
Justiziar, Leiter Recht, Bundesverband Digitale Wirtschaft (BVDW) e.V.

Gregor Rackwitz,
Ad Technology Manager, Bauer Advertising KG

Tobias Wegmann,
CTO, mediascale GmbH & Co. KG,
stv. Vorsitzender der Fokusgruppe Targeting im BVDW

September 2015