Hochschule Kempten

Fakultät Informatik

Seminararbeit

Tracking von Benutzerverhalten durch Cookies

Johannes Börmann

Gutachter(in):	Georg Hagel; Alexander Bartel
Verfasser:	Johannes Börmann
Matrikel-Nr.:	326925
Adresse:	Marktplatz 6, 87671 Ronsberg
E-Mail:	johannes.f.boermann@stud.hs-kempten.de
Eingereicht:	04. Juli 2018

Kurzzusammenfassung

In dieser Arbeit wird das Benutzertracking mit Hilfe von Cookies im Internet näher betrachtet. Es wird erläutert, was Cookies sind und welche Einsatzmöglichkeiten zum Tracken sich durch diese ergeben. Dabei wird der Fokus auf die Unterscheidung zwischen First und Third Party Tracking gelegt. Hervorgehoben werden auch speziellere Fälle, wie die von Facebook und Google. Die Schutzmaßnahmen, um sich gegen Benutzertracking im Internet zu wehren sind außerdem Bestandteil dieser Arbeit. Es wird zudem ein Ausblick aufgezeigt, ob Cookies auch in Zukunft noch Bestand haben werden.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Heutzutage funktioniert es nicht, Aktivitäten im Internet zu erledigen, ohne sichtbare Spuren zu hinterlassen. Es gibt verschiedene Technologien, um Benutzer bei ihren Aktivitäten im Internet zu verfolgen. Zu einer der beliebtesten Technologie im Desktopbereich gehören dabei auch die kleinen Datenpakete, die sogenannten Cookies. Cookies bieten weitreichende Möglichkeiten, den oft nichtsahnenden User bei seinen Interaktionen im Internet zu tracken. Viele Menschen sind oft verwundert, wenn sie auf Internetseiten plötzlich Werbung geschaltet bekommen, die exakt zu den Themen passt, über die sie sich in letzter Zeit oft im Internet informiert haben. Wie etwas derartiges funktioniert und was genau Cookies damit zu tun haben, wird in dieser Arbeit näher erläutert.

1.1 Ziel der Arbeit

Ziel dieser Arbeit ist es herauszufinden, wie User mit Hilfe von Cookies im Internet getrackt werden können. Dabei wird genauer auf die verschiedenen Möglichkeiten eingegangen, die mit Hilfe von Cookies zum Einsatz kommen. Auf Basis dieser Erkenntnisse wird anschließend geprüft, inwieweit man sich gegen dieses Tracking wehren kann und inwiefern sich dies auf die User Experience im Internet auswirkt.

1.2 Was sind Cookies

Zunächst sollte geklärt werden, was Cookies überhaupt sind. Cookies sind kleine Datenpakete, die von der Webseite, die man besucht, auf dem Rechner gespeichert werden [1]. Cookies speichern Informationen, wie z.B. die bevorzugte Sprache oder andere persönliche Seiteneinstellungen. Wenn diese Webseite später erneut besucht wird, übermittelt der Browser die gespeicherten Cookie-Informationen an die Seite zurück. Dadurch können individuelle und auf den User zugeschnittene Informationen angezeigt werden [1]. Grundsätzlich sind Cookies also dazu gedacht, dem Benutzer den Umgang im Internet zu erleichtern [7]. Sie ermöglichen es zum Beispiel, dass man beim Onlineeinkauf seinen Warenkorb bestücken kann, ohne dass man sich auf jeder Unterseite eines Händlers neu als ein und derselbe Kunde zu erkennen geben muss [3].

Im nachfolgenden Screenshot ist eine Übersicht der Cookies zu sehen, die beim Laden von www.focus.de auf dem Rechner gespeichert werden.

Die Hauptbestandteile eines Cookies sind der *Name*, der *Wert* und die *Domain*. Der

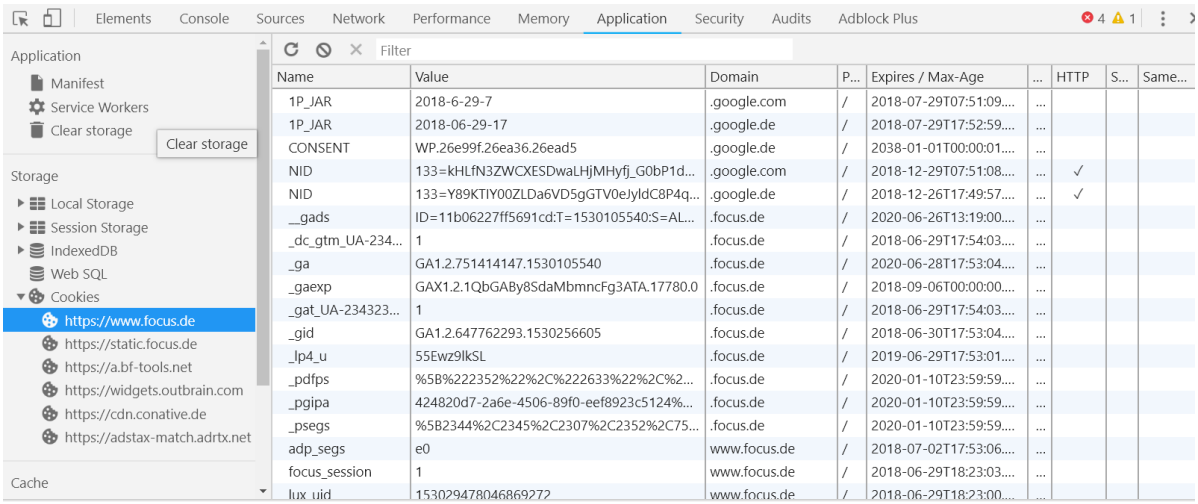

Abbildung 1.1: Cookies: Inhalt

Name ist die Bezeichnung des jeweiligen Cookies und der Wert beinhaltet Informationen, die nur für Maschinen lesbar sind. Dieser Wert könnte beispielsweise eine User-ID beinhalten, die den User beim Aufruf einer bestimmten Webseite eindeutig identifizieren kann [10]. Die Domain gibt an, von welcher Seite das jeweilige Cookie stammt bzw. wer es gesetzt hat.

Ein Cookie beinhaltet außerdem noch weitere Informationen. Erwähnenswert ist hierbei das so genannte *Expire Date*. Dieses legt fest, zu welchem Zeitpunkt das Cookie wieder automatisch vom Rechner gelöscht wird.

1.3 Problemstellung

Ursprünglich sollten Cookies nur kurzzeitig und zwar für die Dauer der aktuellen Verbindung gespeichert und danach wieder gelöscht werden, wovon in der Praxis aber abgegangen wurde, sodass Cookies von Seiten des Web-Anbieters zum Teil gar nicht mehr entfernt werden [7]. Auch die Annahme, dass nur der Web-Anbieter, der das Cookie auf dem Rechner des Nutzers platziert hat, auf dieses Zugriff hat, ist nicht richtig [7]. Der Anbieter ist in der Lage, die Zugriffsrechte auf andere auszudehnen, so dass sich auch Dritte die Cookies zu Nutze machen können [7]. Dieses Szenario hat zur Folge, dass diverse Drittanbieter sich nun Zugriff auf Informationen von den Benutzern verschaffen

können, um daraus Datenprofile zu erstellen. Diese Datenprofile werden in der Praxis häufig verkauft bzw. dazu verwendet, dem Benutzer spezifische Werbung präsentieren zu können [7]. Vor allem sogenannte Advertising-Rings oder Werbeverbünde sind darauf aus, Nutzerprofile zu erhalten, um diese dann zu wirtschaftlichen Zwecken weiterzuverwenden [7]. Ein sehr bekanntes Beispiel dafür ist im Advertising Bereich der Anbieter *Doubleclick*[1].

Das Problem besteht hauptsächlich darin, dass die meisten Nutzer gar nicht wissen, wer die Informationen sammelt und um welche es sich überhaupt handelt. Sie wundern sich oft darüber, dass Webseiten plötzlich auf sie zugeschnittene Werbung zeigen können, ohne dass sie dort jemals etwas über ihre Vorlieben Preis gegeben haben. Als Beispiel eignet sich Facebook dazu am besten: Fast jeder Nutzer wurde schon einmal davon überrascht, wenn er plötzlich auf Facebook genau die Kategorie von Seiten vorgeschlagen bekommt, die zu seinem Browsing Verlauf im Internet passen. Wenn man sich beispielsweise im Internet nach neuen Schuhen umgeschaut hat, ist es nicht selten der Fall, dass man beim nächsten Facebook Besuch die Seite der Firma Zalando vorgeschlagen bekommt. Dies ist aber noch eine der etwas harmloseren Varianten von Benutzertracking im Internet. Weitaus problematischer kann es werden, wenn Tracking- bzw. Advertising Unternehmen plötzlich Informationen über sehr viel sensiblere Daten des Nutzers erhalten. Beispiele hierfür sind das Aufsuchen von Seiten über Pornographie, medizinische Informationen, wie etwa über schwere Krankheiten (AIDS, Krebs), politische Gesinnungen, etwa über rechtsextreme Inhalte oder religiöse Themen, wie z.B. bestimmte Sekten [7]. Denn genauso wie bei Shoppingseiten können durchaus Cookies von Drittanbietern auf Seiten, auf denen man sich über eine Krankheit informiert, gesetzt werden. Prinzipiell lassen Cookies keinerlei Rückschlüsse auf die Person, die hinter dem Rechner sitzt, zu. Bedenklich wird es aber, wenn Unternehmen wie Facebook, Google etc. diese Daten mit realen Personen in Verbindung bringen können. Auch wenn Google behauptet, dass sie mit ihren Diensten keine Profile über den Gesundheitszustand oder der politischen Einstellung generieren [9], lässt sich das natürlich nicht mit absoluter Sicherheit ausschließen. Um der Frage auf den Grund zu gehen, inwieweit man sich vor diesen Trackingmechanismen schützen kann und inwiefern sich diese Schutzmaßnahmen auf die User-Experience im Internet auswirken, werden zunächst die Arten von Cookies und die daraus entstandenen Trackingszenarien näher betrachtet.

[1] Online Marketing Unternehmen von Google

2 Arten von Cookies

Bevor man detaillierter auf die verschiedenen Arten des Trackings durch Cookies eingeht, sollte erst einmal ein Grundverständnis darüber vorliegen, inwiefern sich Cookies voneinander unterscheiden können. Grundsätzlich lassen sich Cookies nach drei Arten unterscheiden:

1. Lifetime
2. Origin
3. Others

2.1 Lifetime

Wie der Begriff schon vermuten lässt, werden die Cookies hierbei über ihre Lebensdauer unterschieden. Es existieren einerseits die so genannten **Session Cookies** und andererseits die **Persistent Cookies**.
Session Cookies sind die Arten von Cookies, die nur temporär gespeichert werden und nach dem Schließen des Browsers wieder gelöscht werden. Diese sind, was den gewohnten Komfort heutzutage im Internet angeht, unabdingbar. Denn gäbe es sie nicht, müsste ein Nutzer bei jedem Seitenwechsel innerhalb einer Webseite seine Informationen erneut übertragen. Am Beispiel eines Einkaufswagens lässt sich das sehr gut verdeutlichen: Wenn ein Nutzer einen Artikel in einen Warenkorb legt und anschließend eine andere Seite aufruft um einen neuen Artikel anzusehen, wäre dieser ohne die Verwendung von Session Cookies wieder verschwunden [2]. Dies hätte natürlich erhebliche Komforteinbußen, die man in der heutigen Zeit nicht gerne in Kauf nehmen möchte.
Persistent Cookies hingegen sind die Arten von Cookies, die dauerhaft auf dem Rechner gespeichert werden. Sie werden erst wieder entfernt, wenn der User diese manuell löscht oder das jeweilige *Expire Date* des Cookies abgelaufen ist. Bei diesen Cookies ist es oft der Fall, dass sie sich monate- oder sogar jahrelang im Browser des Benutzers befinden. Es gibt keine rechtliche Begrenzung dieses *Expire Dates*, allerdings begrenzen viele Unternehmen dieses mittlerweile von sich aus auf eine bestimmte Zeit. Google hat

beispielsweise im Jahr 2007 angekündigt, die maximale Lebenszeit ihrer Cookies auf zwei Jahre zu begrenzen. Bis zu diesem Zeitpunkt war das *Expire Date* bei vielen Cookies auf das Jahr 2038 gesetzt. Begründet wurde das Ganze durch eine „Erhöhung der Privatsphäre“ für den Anwender [8].

2.2 Origin

Cookies können außerdem nach ihrer Herkunft unterschieden werden. Dieses Verständnis darüber ist essentiell in Bezug auf die verschiedenen Trackingszenarien, die im darauffolgenden Kapitel näher beschrieben werden.

First Party Cookies

First Party Cookies sind die Arten von Cookies, die von der Webseite, die man aufruft auf dem Rechner gespeichert werden. Ruft man beispielsweise über seinen Browser *www.focus.de* auf, so werden beim Ladevorgang eine Vielzahl von Cookies gesetzt (vorrausgesetzt die Browsereinstellungen lassen dies zu). Hierbei bezeichnet man nun alle Cookies als First Party Cookies, welche als Domain (siehe Kapitel 1.2) *focus.de* beinhalten. Das bedeutet, dass diese Cookies direkt von der Webseite stammen, die man aufruft.

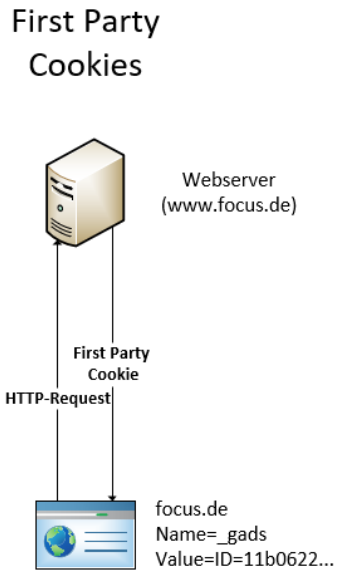

Abbildung 2.1: Cookies: First Party Cookies, in Anlehnung an: [13]

Third Party Cookies

Beim Ladevorgang einer Webseite kann es auch häufig passieren, dass nicht nur Cookies explizit von dieser Seite gesetzt werden, sondern auch welche von Drittanbietern. Diese stammen nicht von der Webseite, die man aufgerufen hat, sondern von externen Anbietern. Möglich gemacht wird so etwas beispielsweise durch das Einbinden von Werbebannern oder diversen PlugIns, die andere Webseiten zur Verfügung stellen. In diesem Beispiel ist zu sehen, wie das Unternehmen *Doubleclick* ein Drittanbieter Cookie beim Laden der Webseite *www.focus.de* setzt. Dieses Cookie wird von nun an bei jedem Aufruf einer Internetseite, die bestimmte Dienste von *www.doubeclick.net* beinhaltet, mitgeschickt. Hier lässt sich also schon zum ersten Mal sehr gut erkennen, welche Potentiale Third Party Cookies mit sich bringen.

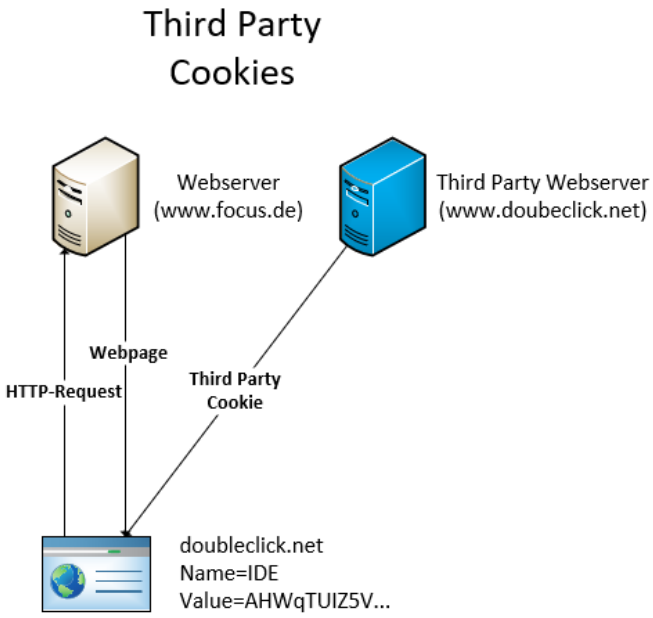

Abbildung 2.2: Cookies: Third Party Cookies, in Anlehnung an: [13]

Im folgenden Screenshot soll diese Unterscheidung noch einmal deutlich gemacht werden, indem analysiert wird, wie sich diese Cookies beim Aufruf von *www.focus.de* im Browser zu erkennen geben:

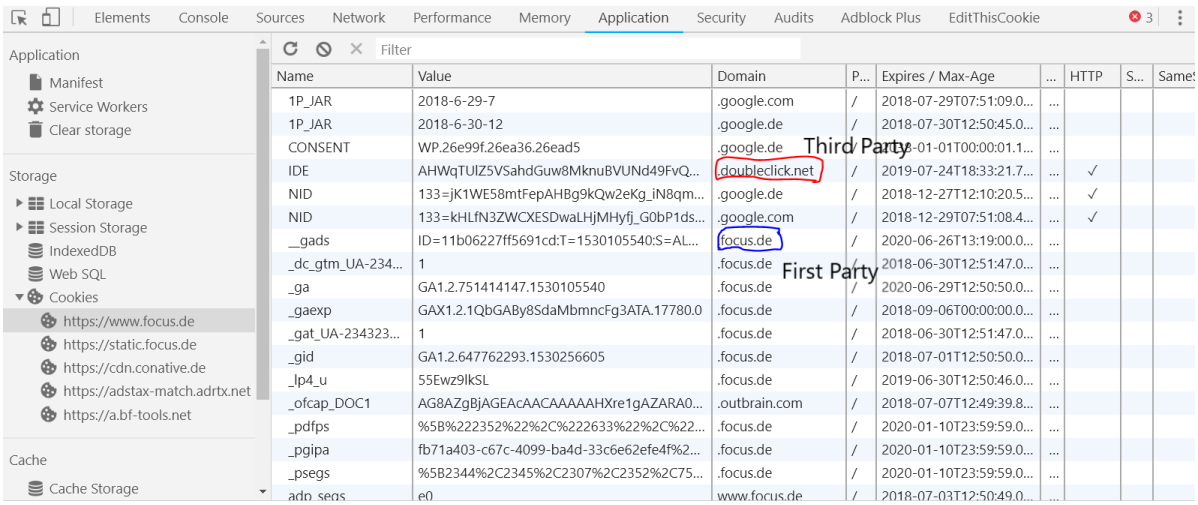

Abbildung 2.3: Cookies: First u.Third Party

2.3 Others

Abgesehen von der Herkunft und der Lebensdauer von Cookies, gibt es noch einige andere Spezialarten, die im Rahmen dieser Arbeit aber nur kurz erwähnt werden:

Supercookies
Unter Supercookies versteht man die Art von Cookies, die als Herkunft eine Top-Level Domain hinterlegt haben. Das bedeutet beispielsweise, dass ein Cookie dieser Art als Domain *.com* besitzt. Sicherheitstechnisch sind diese Cookies extrem bedenklich, da diese an jede Webseite, die mit *.com* endet, geschickt werden.

Securecookies
Securecookies sind Cookies, die nur über eine gesicherte HTTP Verbindung übertragen werden können (HTTPS).

Darüber hinaus gibt noch viele weitere Arten von Cookies, die oft ausschließlich für ihr ganz bestimmtes Einsatzgebiet entwickelt wurden.

3 Tracking Szenarien

Nachdem im vorherigen Kapitel die unterschiedlichen Arten von Cookies näher erläutert wurden, wird nun untersucht, welche Einsatzpotentiale sich daraus ergeben können, um den Nutzer im Internet zu tracken.

3.1 Third Party Tracking

Mit Hilfe von Third Party Cookies wird es Unternehmen sehr einfach gemacht, den User webseitenübergreifend zu tracken. Wie im vorherigen Beispiel schon deutlich gemacht, wird beim Aufruf einer Webseite oft eine Vielzahl an Third Party Cookies gesetzt. Nun gehe man von folgendem Beispiel aus:
Ein User hat einen komplett neu aufgesetzten Browser, der noch keinerlei Cookies gespeichert hat. Nun ruft er zum ersten Mal eine Webseite auf, die Werbung oder ähnliches eingebunden hat und bekommt unwissend neben den First Party Cookies noch einige Third Party Cookies auf seinen Rechner gespeichert. Im Beispiel weiter oben wurde dabei das Third Party Cookie von *Doubleclick* verwendet und soll auch hier weiter zur Veranschaulichung dienen. Surft der Anwender nun weiter und trifft auf andere Webseiten, die den selben Dienst von *Doubleclick* eingebunden haben, so sieht das Szenario folgendermaßen aus: Beim Anfragen einer Webseite wird der Seiteninhalt rekursiv geladen und zwar so lange, bis alle Inhalte heruntergeladen wurden. Sollte ein Teil dieses Inhaltes zum Beispiel auch von *Doubleclick* stammen, so schickt der Browser beim Ladevorgang automatisch das zuvor auf dem Rechner gespeicherte Cookie dorthin. Anhand einer nutzerspezifischen ID, die im Cookie hinterlegt ist, weiß *Doubleclick* also genau, wer diese Seite aufgerufen hat und wo er zuvor schon überall war. Wenn man dieses Szenario nun weiterspinnen möchte, stellt man fest, dass dadurch über einen längeren Zeitraum ein sehr genauer Browsingverlauf des Benutzers erstellt werden kann. *Doubleclick* nutzt dies dazu, um herauszufinden, welche Werbung am besten zu dem jeweiligen User passt, um diese dann dynamisch generiert anzeigen zu lassen. Dies erklärt auch, warum viele Benutzer im Internet genau die Werbung zu den Themen zu Gesicht bekommen, über die sie sich in letzter Zeit im Internet informiert haben. Neben Google's *Doubleclick* existieren noch viele weitere Online-Marketing Unternehmen, die sich auf

gezielte Werbeschaltungen spezialisiert haben. Erwähnenswert ist an dieser Stelle noch *Outbrain*, dessen Service auf sehr vielen bekannten Nachrichtenportalen, wie zum Beispiel *www.cnn.com*, zu finden ist.
Um an einen besonders ausführlichen Browsingverlauf eines Nutzers zu gelangen, ist es notwendig, möglichst viele Daten über ihn sammeln zu können. Deshalb haben die Adverstisingunternehmen, die auf möglichst vielen und vorallem bekannten Webseiten eingebunden sind, die besten Möglichkeiten, Profile über die Benutzer zu erstellen. Aufgrund dessen versuchen Unternehmen oftmals, über diese großen Marketing-Unternehmen ihre Werbung platzieren zu lassen, da sie erstens auf sehr vielen Webseiten vertreten sind und zweitens genau den Usern die Werbung zeigen können, die auch auf sie zutrifft.

3.2 Advertising Networks

Mittlerweile haben sich im Internet auch so genannte *Advertising Networks* gebildet. Das bedeutet, dass ein Third Party Advertiser wie *Doubleblick* oder im nachfolgenden Beispiel gezeigten *www.admeld.com* seine Informationen (Cookies) an diverse weitere Dienste weitergibt. Die folgende Grafik soll dieses Szenario verdeutlichen:

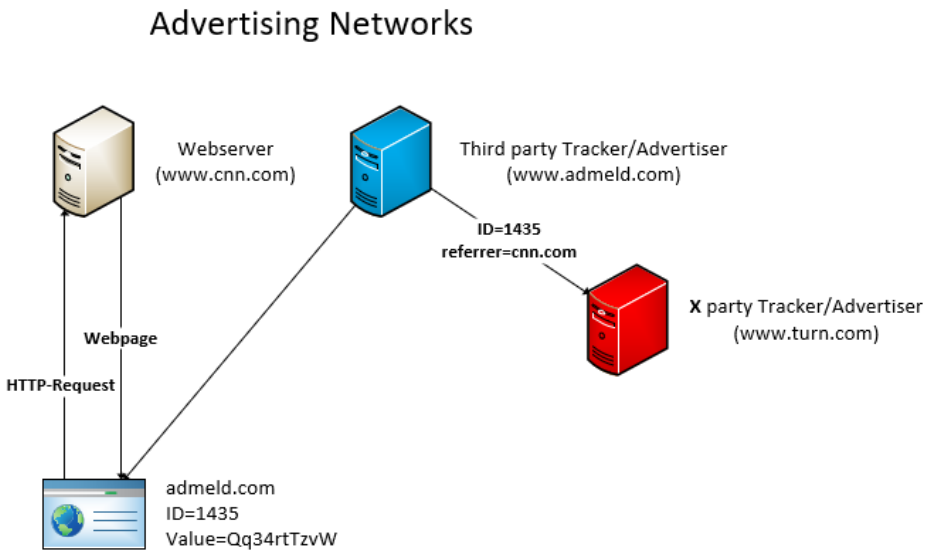

Abbildung 3.1: Advertising Networks, in Anlehnung an: [13]

Hier wird es problematisch. Der Nutzer hat keinerlei Möglichkeit mehr nachzuvollziehen, was mit seinen Cookies passiert bzw. wer alles an die Informationen gelangt, welche Webseite er besucht hat. Die Advertisingunternehmen im Hintergrund verlassen sich

vollkommen auf die Informationen, die ihnen von den Third Party Advertisern geliefert werden und müssen selbst nicht in eine Webseite eingebunden werden [13]. Es existieren leider sehr wenige Informationen über diese *Advertising Networks*, da man, wie schon gezeigt, nicht feststellen kann, wer dort alles involviert ist und wohin diese Informationen überall weitergeleitet werden [13]. Vermuten lässt sich aber, dass sich im Hintergrund eine sehr große Anzahl an Online-Advertisern zusammengeschlossen hat, die sich gegenseitig mit ihren Informationen austauschen, um eine sehr große Informationsgewinnung zu erlangen.

3.3 Third Party Analytics

Abgesehen von der Advertising Richtung existieren auch Unternehmen, die Dienste bereitstellen, um diverse Analysen auf Webseiten durchzuführen. Das weitaus bekannteste Beispiel hierfür ist *Google Analytics*. Viele Webseitenbetreiber nutzen diesen Dienst von Google auf ihrer Webseite, um Informationen zur Besucheranzahl oder das Verhalten der Besucher auf der Webseite zu analysieren. Dabei ist unbedingt folgendes zu unterscheiden: Third Party Analytics bedeutet nicht gleich, dass Google in diesem Fall Third Party Cookies nutzt, um diesen Dienst anbieten zu können. Der Ablauf sieht in diesem Fall folgendermaßen aus:

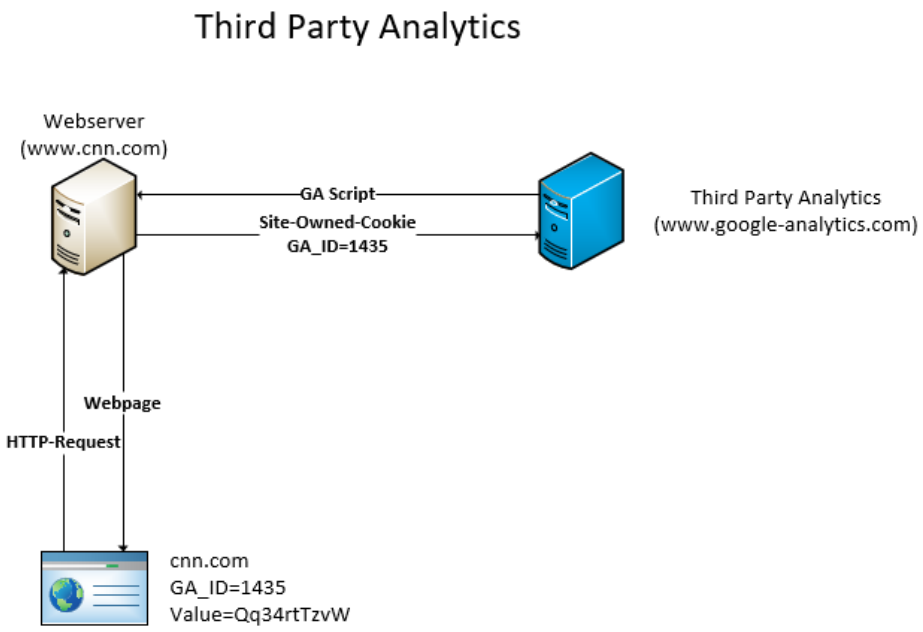

Abbildung 3.2: Third Party Analytics: GA, in Anlehnung an: [13]

Die jeweilige Webseite, die den Dienst von Google nutzt, hat ein Google Analytics Script eingebunden. Dieses Skript wird auf der Webseite selbst ausgeführt, um bestimmte Daten zu tracken. Aufgrund der *same-origin-policy* ist dieses Skript nur dazu in der Lage ein First Party Cookie, welches von der Webseite selbst stammt, zu setzen. Da Google aber auf irgendeine Art und Weise an diese gesammelten Daten kommen muss, um Auswertungen vorzunehmen, werden diese in den HTTP-Request Parametern an *google-analytics.com* zurückgesendet [4].
Dadurch, dass in diesem Fall nur First Party Cookies verwendet werden, die von der jeweiligen Webseite stammen, kann Google einen Benutzer mit diesem Dienst nicht domainübergreifend verfolgen. Besucht ein Benutzer eine andere Webseite, die auch ein Skript von Google Analytics beinhaltet, bekommt er eine neue ID von dieser Webseite im Cookie hinterlegt, die Google nicht in Verbindung bringen kann mit anderen Webseitenbesuchen des selben Nutzers. Zusammenfassend lässt sich hier also sagen, dass Google Analytics, was das Tracking angeht, noch eine der harmloseren Varianten darstellt.

3.4 Sonderfall Facebook

Immer wieder wird in den Medien darüber berichtet, mit welchen ausgefeilten Methoden Facebook versucht, die Nutzer zu tracken. So berichtete auch die Welt am 09.03.2016 beispielsweise über das Tracking per Like Button[1]. Was das mit den Cookies zu tun hat und welche Besonderheit Facebook sich hier zu nutzen macht, wird im Folgenden näher erläutert.
In Kapitel 3.1 wurde bereits beschrieben, wie mit Hilfe von Third Party Cookies gezielt Werbung geschaltet und der Nutzer webseitenübergreifend getrackt werden kann. Dieses Prinzip macht sich auch Facebook grundlegend zu Nutze. Bei sehr vielen Webseiten war es bis vor kurzem noch so, dass diese häufig diverse PlugIns von Facebook eingebunden haben. Das könnte beispielsweise ein Like-Button sein, mit dem man direkt per Mausklick die Facebookseite der Homepage liken kann:

Abbildung 3.3: Facebook Like Button

Hat sich ein Benutzer irgendwann einmal bei Facebook eingeloggt, so bekommt er von

[1] https://www.welt.de/wirtschaft/webwelt/article153117319/Der-Facebook-Daumen-ist-ein-raffinierter-Spion.html, zuletzt abgerufen am: 03.07.2018

Facebook selbst ein First Party Cookie gesetzt. Nun ist es aber so, dass wenn dieser Benutzer sich durch das Internet bewegt und auf Seiten trifft, die beispielsweise diesen Like Button eingebunden haben, das First Party Cookie von Facebook beim Ladevorgang dieses PlugIns an Facebook gesendet wird [11]. Das bedeutet zum einen, dass Facebook, genau wie die anderen Advertising Unternehmen, die Möglichkeit hat, den Benutzer webseitenübergreifend zu tracken. Zum anderen besteht aber hier die Besonderheit darin, dass es sich nicht um Drittanbietercookies handelt, sondern um **First Party Cookies**. Dies ist eine sehr wichtige Unterscheidung, die man verstehen sollte. Facebook ist in diesem Szenario also ein Third Party Tracker, der sich aber seine eigenen First Party Cookies zu Nutze machen kann [13]. Die Konsequenzen, die sich daraus ergeben, sind enorm. Auch wenn vorsichtigere Benutzer Third Party Cookies durch die entsprechenden Browsereinstellungen verweigern, hat Facebook immer noch die Möglichkeit die Nutzer weiterhin zu tracken. Das unterscheidet Facebook extrem von anderen„herkömmlichen“ Advertisern. Dies ist auch eine Sache, der sich sehr viele Nutzer sicherlich nicht bewusst sind.
Facebook hat in diesem Fall den großen Vorteil, dass sich eine Menge User direkt dort anmelden und sich ein First Party Cookie setzen lassen. Gleichzeitig ist die Einbindung von Facebook PlugIns auf vielen Webseiten sehr verbreitet. Advertising Unternehmen wie *Doubleclick* könnten sich diese Methodik nur sehr schwer zu nutzen machen, da die wenigsten Besucher *www.doubleclick.net* direkt besuchen, um sich ein solches First Party Cookie setzen lassen zu können. Sie sind weiterhin stark auf Third Party Cookies angewiesen.
Die Besonderheit an dem Like Button ist außerdem, dass es ausreicht, dass dieser beim Seitenaufruf gerendert wird, um Informationen an Facebook zu übermitteln. Er muss nicht einmal angeklickt werden. Heutzutage ist diese Form der Like Buttons nicht mehr so oft zu sehen, da durch neue Datenschutzbestimmungen, vor allem auch in Bezug auf die DSGVO, die Weitergabe von personenbezogenen Daten an Drittanbieter ohne Einwilligung rechtlich nicht abgesegnet ist [6].

Nichtsdestotrotz sollte ein Grundverständnis darüber herrschen, welche verschiedenen Möglichkeiten zum Benutzertracking mit Hilfe von Cookies ausgeschöpft werden können. Denn nicht nur Facebook, sondern auch andere große Unternehmen wie Twitter, Google und co. nutzen die Möglichkeiten von so genannten *Social Widgets*. Bei diesen Social Media Anbietern gibt es außerdem noch einen weit besorgniserregenderen Aspekt, als bei den herkömmlichen Advertisingunternehmen. Sie besitzen oft das Privileg, dass

Benutzer mit ihren echten persönlichen Daten dort registriert sind. Marketing Unternehmen wie *Doubleclick* haben selten die Möglichkeit einen Personenbezug herzustellen. Bei diesen Firmen wird der User über eine eindeutige ID oder auch über seine IP-Adresse identifiziert. Die Social Media Anbieter hingegen sind in der Lage, die getrackten Informationen einer realen Person zuzuordnen. Für die möglichen Folgen, die sich daraus ergeben können, wird hiermit auf die Problemstellung in Kapitel 1.2 verwiesen.
Dass den großen Unternehmen wie Facebook der Datenschutz seiner Nutzer nicht besonders am Herzen liegt, kann man sehr gut am aktuellen Datenmissbrauchsfall, in welchem Facebook persönliche Daten an *Cambridge Analytica*[2] weitergegeben hat, erkennen. Dabei handelt es sich um geschätzte 87 Millionen Betroffene Benutzer[3]. Dieser Datenskandal zeigt zum ersten Mal eine Dimension auf, die man sich wahrscheinlich so hätte nicht vorstellen können.

[2]Britisches Datenanalyseunternehmen, welches im Facebook Skandal involviert war
[3]http://www.sueddeutsche.de/digital/datenmissbrauch-was-ist-eigentlich-gerade-bei-facebook-los-1.3932349, zuletzt abgerufen am: 03.07.2018

4 Schutzmechanismen

Nachdem erläutert wurde, welche Arten von Cookies es gibt und wie verschiedene Trackingszenarien aussehen, soll auch der Punkt wie man sich gegen das Tracking schützen kann, nicht außer Acht gelassen werden. Es wird hier einerseits auf die technischen Schutzmaßnahmen im Browser eingegangen und andererseits auf das persönliche Verhalten im Internet.

4.1 Browsereinstellungen

Blockieren von Third Party Cookies
Der wohl bekannteste als auch grundsätzlichste Ansatz ist es, über die Browsereinstellungen das Zulassen von Third Party Cookies zu unterbinden. Jeder moderne Browser bietet heutzutage diese Möglichkeit an. Mit Hilfe dieser Einstellung lassen sich die in Kapitel 3.1 und 3.2 beschriebenen Trackingszenarien sehr gut einschränken. Wenn Drittanbietercookies geblockt werden, sind die Advertisinganbieter meist nicht mehr in der Lage, über die Webseiten anderer derartige Cookies zu hinterlegen, um die User zu tracken.
Diese Option hat außerdem den Vorteil, dassn die User Experience im Internet fast nicht beeinträchtigt wird. Auch wenn Third Party Cookies geblockt sind, bleiben fast alle Webseiten genauso gut benutzbar wie zuvor. Hierbei handelt es sich also um eine sehr einfache und effiziente Möglichkeit, gegen das Tracking vorzugehen. Wie das Blocken von Third Party Cookies in dem jeweiligen Browser funktioniert, ist der entsprechenden Herstellerseite zu entnehmen. Im Regelfall ist diese Funktion zwar etwas versteckt, aber mit den passenden Informationsquellen auf jeden Fall zu finden.

Blockieren von First Party Cookies
Da im letzten Absatz über das Blocken von Third Party Cookies gesprochen wurde, soll auch eine etwas drastischere Variante, nämlich das Blockieren aller Cookies, nicht außer Acht gelassen werden. Die meisten Browser bieten zusätzlich die Möglichkeit, auch First Party Cookies zu blockieren. Nutzt man diese Einstellung, so ist man praktisch von allen Arten von Cookies befreit. Allerdings sollte man sich in diesem Fall unbedingt den

Konsequenzen bewusst werden, die daraus entstehen.
Cookies wurden grundsätzlich dafür entwickelt, um dem User den Umgang im Internet zu erleichtern [7]. Vor allem First Party Cookies, die direkt von der jeweiligen Webseite stammen, bringen dabei oft sehr viele nützliche Funktionen mit sich. Diese wurden bereits in Kapitel 1.1 näher erläutert. Blockiert der User nun diese Cookies, kann dies enorme Auswirkungen auf seine Experience im Internet haben[5]. Um ein paar Beispiele aufzuzeigen, eignen sich bekannte Unternehmen wie Amazon und Facebook dazu am besten:
In beiden Testfällen wurde der Browser Google Chrome (Version: 67.0.3396.99, 64 Bit) verwendet, in welchem alle Arten von Cookies über die Einstellungen blockiert werden. Auf *www.amazon.de* wurde in diesem Szenario versucht einen Artikel auszuwählen und diesen in den Warenkorb zu hinterlegen. Das Resultat sieht folgendermaßen aus:

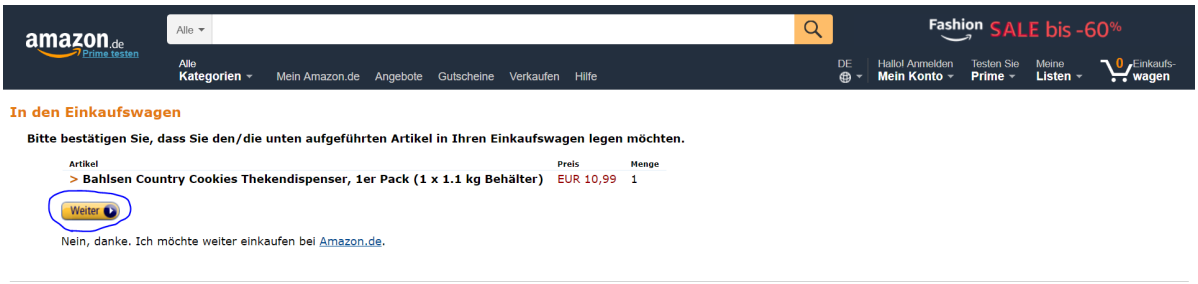

Abbildung 4.1: Amazon Einkauf bei deaktivierten Cookies

Man ist nur noch in der Lage bis zu diesem Bildschirm zu gelangen, in dem Amazon möchte, dass man die Hinterlegung in den Warenkorb bestätigt. Diesen Button kann man aber drücken so oft man will, es passiert nichts weiter. Das bedeutet letztendlich, dass man durch das Deaktivieren aller Cookies keine Chance mehr hat, auf Amazon etwas zu bestellen. Was außerdem gefährlich werden kann, ist die Tatsache, dass der Nutzer hier keinerlei Hinweise darauf bekommt, warum dieser Vorgang nicht mehr funktioniert. So könnte es beispielsweise passieren, dass der Anwender lange Zeit sehr gut ohne Cookies durch das Internet navigieren kann, aber dann doch irgendwann der Fall auftritt, dass Seiten komisch reagieren und er nicht mehr nachvollziehen kann, woran das liegt.
Bei *www.facebook.com* sieht das Szenario ähnlich aus, nur mit dem Unterschied, dass der User hier direkt darauf hingewiesen wird, seine Cookies zu aktivieren. In Abbildung 4.2 ist das Ergebnis zusehen, welches man erhält, wenn man sich ohne Cookies versucht bei

Facebook einzuloggen.

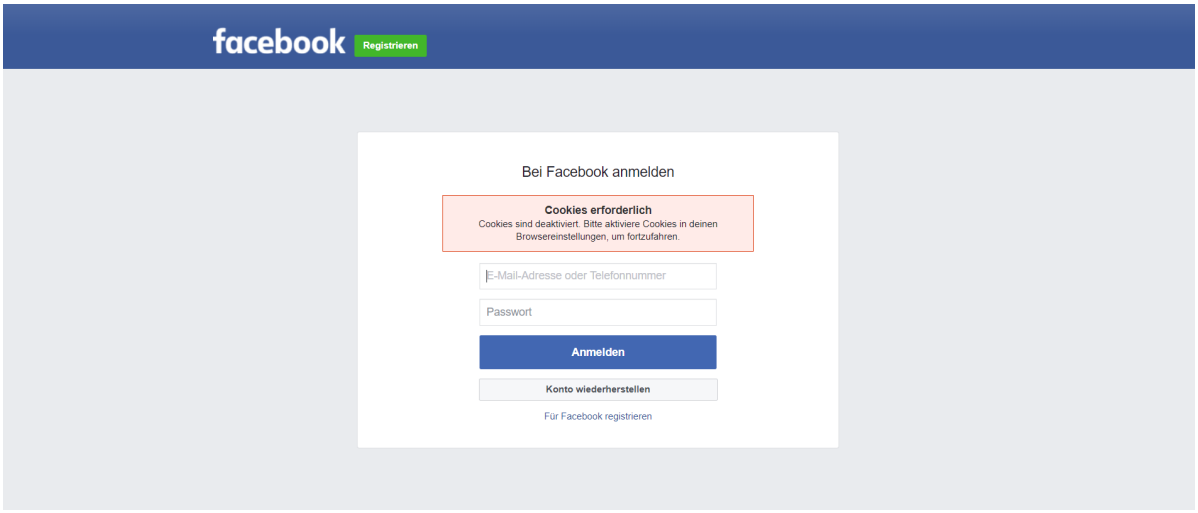

Abbildung 4.2: Facebook Login bei deaktivierten Cookies

In diesem Fall wurden bewusst zwei „Extrembeispiele“ gewählt, um aufzuzeigen, welche Konsequenzen das Deaktivieren von First Party Cookies mit sich bringen kann. Es gibt natürlich auch andere Internetseiten, auf denen man sich problemlos ohne Cookies bewegen kann. Diese sind aber im heutigen Zeitalter eher eine Seltenheit. Das bedeutet, dass man sich sehr gut darüber im Klaren sein sollte, welche Risiken das Blockieren von allen Cookies mit sich bringt.

Damit man einen Überblick darüber bekommt, wie in modernen Browsern standardmäßig mit Cookies umgegangen wird, wurden in der folgenden Tabelle die Standardeinstellungen der vier bekanntesten Browser gegenübergestellt:

	First Party Cookies	**Third Party Cookies**
Google Chrome	Alle	Alle
Mozilla Firefox	Alle	Mit Einschränkung*
Safari	Alle	Mit Einschränkung*
Microsoft Edge	Alle	Fast alle**

Tabelle 4.1: Moderne Browser: Standardeinstellungen Cookies

/*Alle Third Party Cookies, die der „P3P compact policy“ entsprechen[1]
/**Nur erlaubt, wenn die Domain schon einmal zuvor ein First Party Cookie gesetzt hat

[1]Für weitere Informationen dazu siehe: https://www.w3.org/P3P/2003/03-compact.html, zuletzt abgerufen am: 03.07.2018

Die Umsetzung, die Microsoft bei ihren Standardeinstellungen in Bezug auf Third Party Cookies gewählt hat, ist als sehr sinnvoll einzustufen. In diesem Fall kann es nicht passieren, dass wie in Kapitel 3.1 beschrieben, *Doubleclick* ein Cookie beim Besuch von *www.focus.de* gesetzt wird, wenn der Benutzer *Doubleclick* zuvor noch nie direkt besucht hat. Was aber außerdem ersichtlich wird ist, dass Third Party Cookies bei allen Browsern nicht standardmäßig komplett blockiert werden. In diesen Fällen ist immer ein manuelles Eingreifen des Users erforderlich.

4.2 User Awareness

Unabhängig von den technischen Maßnahmen, die man zum Schutz gegen das Tracking anwenden kann, spielt auch das Bewusstsein des jeweiligen Users bei seinen Aktivitäten im Internet eine sehr große Rolle. So sollte sich beispielsweise jeder selbst sehr gut überlegen, ob er Dienste wie Facebook, Google, Twitter etc. wirklich in Anspruch nehmen möchte. Denn wie in Kapitel 3.4 beschrieben, sind diese Anbieter meistens in der Lage, nicht nur die User zu tracken sondern diese getrackten Informationen mit einer realen Person in Verbindung zu bringen. Jeder sollte sich darüber im Klaren sein, dass diese Dienste zum Beispiel in der Lage sind, Profile über den Gesundheitszustand oder andere sensible Persönlichkeitsprofile zu erstellen[2]. Sollten diese Daten auf irgendeinem Weg zum Beispiel an die Krankenkassen oder andere Institutionen gelangen, so wären die Folgen, die sich daraus ergeben, erheblich.

4.3 Zusammenfassung

Um sich gegen das Benutzertracking im Internet durch Cookies zu wehren wurden einerseits die technischen Möglichkeiten angeschnitten und auf der anderen Seite wurde das menschliche Bewusstsein in Sachen Internetnutzung etwas näher erläutert. Zusammenfassend ist zu empfehlen, sich eine solide Mischung aus beidem anzueignen. Das bedeutet, man sollte prinzipiell immer alle Drittanbietercookies durch den Browser blockieren lassen und auch gleichzeitig etwas bewusster durch das Internet navigieren. Insbesondere ist darauf vor allem auf die Dienste zu achten, die mit persönlichen Daten arbeiten. In gewisser Weise ist jeder selbst dafür verantwortlich, wie viele Daten er über sich Preis gibt und wie viel Aufwand man betreiben möchte, um sich gegen das Tracking zu schützen.

[2] http://www.dailyherald.com/business/20180421/analysis-facebook-knows-a-ton-about-your-health-now-it-wants-to-profit-from-that, zuletzt abgerufen am: 03.07.2018

5 Ausblick

Cookies sind eine Technologie, die schon in den frühen 90er Jahren ihren Ursprung fand [12]. Da es schon sehr bemerkenswert ist, dass sich eine Technologie im heutigen Zeitalter so lange gehalten ist, ist es nicht verwunderlich, dass dieser Entwicklung langsam ein Rückgang prognostiziert wird [1]. Dies hat den Grund, dass die Menschen immer mehr auf mobile Endgeräte setzen und immer weniger Aufgaben an dem normalen Desktoprechner erledigen. Auf mobilen Endgeräten gestaltet sich das Tracking durch Cookies als sehr schwierig, da mobile Applikationen eine so genannte „Webview“ nutzen, um Webseiten bzw. Apps darzustellen. Diese Webview speichert zwar auch Cookies ab, aber das Problem besteht darin, dass jeder Browser bzw. jede App eine unterschiedliche Webview oder Sandbox nutzt, um Cookies zu speichern. Das erschwert es ungemein, den User über verschiedene Apps hinweg zu tracken [14].
Die Anbieter der Dienste setzen deshalb immer mehr auf andere Techniken, die, vor allem in Bezug auf mobile Endgeräte, besser zum Tracken geeignet sind. Zwei Beispiele dafür sind:

Universal Login Tracking
Dieses Verfahren gibt es sowohl im Desktop- als auch im mobilen Bereich. Dabei wird darauf abgezielt, dass der Nutzer sich auf möglichst vielen Webseiten mit dem selben Login anmeldet. [11] Einige Beispiele solcher universalen Loginbuttons sind hier dargestellt:

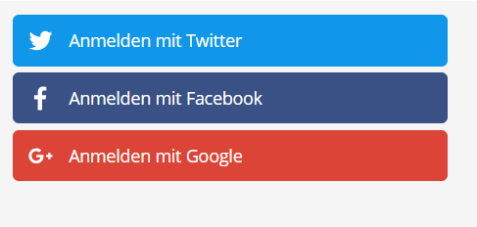

Abbildung 5.1: Universal Logins

[1] https://clearcode.cc/blog/cookie-alternative-future-mobile-advertising/, zuletzt abgerufen am: 03.07.2018

Mit dieser Technik haben Dienste wie Facebook, Google etc. die Möglichkeit, ganz einfach herauszufinden, auf welcher Seite sich der jeweilige User außerhalb ihrer Dienste zusätzlich noch angemeldet hat.

Device Fingerprint
Anbieter versuchen zunehmend, einen so genannten virtuellen „Fingerabdruck“ zu erstellen, der ein Gerät, egal ob Desktop- oder mobiles Endgerät, eindeutig identifizieren kann. Dies kann geschehen, indem man verschiedene Informationen, die vom jeweiligen Gerät preisgegeben werden, versucht zu verknüpfen. Darunter fallen beispielsweise Dinge wie der *Gerätetyp*, das *Betriebssystem* und die *IP Adresse* [14].

Ein weiteres Problem ist, dass der Nutzer mit Hilfe von Cookies nicht *geräteübergreifend* getrackt werden kann. Heutzutage ist es sehr wahrscheinlich, dass jemand nicht nur ein Endgerät besitzt, sondern mehrere. Es ist oft der Fall, dass eine Person ein Smartphone, ein Notebook und eventuell noch ein Tablet besitzt. Zudem steigt der Trend, dass neben dem privaten Smartphone noch ein zusätzliches Firmenhandy zum Einsatz kommt.

Zusammenfassend kann man sagen, dass der Rückgang der Nutzung von Desktoprechnern maßgeblich dazu beiträgt, dass das Tracking über Cookies in Zukunft weiter etwas an Relevanz verlieren wird. Natürlich werden Cookies in diesem Bereich weiterhin wie bisher eingesetzt, aber die Dienste werden sich zunehmend mehr auf das Tracking auf mobilen Endgeräten konzentrieren, da in dieser Richtung immer höhere Potentiale entstehen.

6 Fazit

Wie am Anfang dieser Arbeit bereits beschrieben, wurden Cookies ursprünglich zu einem sehr nützlichen Zweck geschaffen, nämlich um den Nutzer bei seinen Aktivitäten im Internet zu unterstützen. Leider haben sehr schnell sehr viele Anbieter die weiteren Potentiale von Cookies erkannt, um diese noch mehr zu ihrem Vorteil nutzen zu können. Aufgrund dessen hat sich innerhalb des letzten Jahrzehntes das Benutzertracking im Internet fast zur Selbstverständlichkeit für viele Unternehmen entwickelt. Für das Ringen nach Daten unter dem auch heute noch bekannten Slogan „*Data is the new oil*“ waren und sind Cookies auch weiterhin eine sehr einfache und effektive Möglichkeit, an Trackingdaten zu gelangen. Viele Anbieter, vor allem im Online Marketing Bereich, haben in dieser Zeit ihr komplettes Geschäftsmodell auf diese Art von Datensammlung ausgerichtet. Für diese zählen Cookies mit zu den wichtigsten Instrumenten.

In Zeiten, in denen Themen wie Datenschutz- und Datensicherheit immer mehr an Bedeutung in der Öffentlichkeit gewinnen, sollte jeder Internetnutzer zumindest darüber aufgeklärt werden, wie er mit Hilfe von Cookies getrackt werden kann und welche Möglichkeiten es gibt, sich gegen solche Techniken zu wehren. Dies wurde in dieser Arbeit anhand von technischen als auch an menschlichen Aspekten versucht zu vermitteln. Der beste Kompromiss um dies zu tun, ist eine gute Mischung aus den technischen- als auch den menschlichen Aspekten zu finden, so dass man immer noch in der Lage ist, sich ohne besondere Einbußen durch das Internet zu bewegen, aber auf der anderen Seite das Tracking so gut es geht einschränkt. Insbesondere wenn das Tracking im Internet mit Personenbezug zusammengeführt wird, sollte sich jeder Mensch darüber im Klaren sein, was das für gravierende Auswirkungen mit sich bringen kann.

Literaturverzeichnis

[1] Cookies - informationen die websites auf ihrem computer ablegen. URL https://support.mozilla.org/de/kb/cookies-informationen-websites-auf-ihrem-computer. Zuletzt abgerufen am 03.07.2018.

[2] URL http://www.allaboutcookies.org/cookies/session-cookies-used-for.html. Zuletzt abgerufen am 03.07.2018.

[3] Internet: Cookies - die wichtigsten fragen. 2012. URL https://www.test.de/Internet-Cookies-die-wichtigsten-Fragen-4343964-0/. Zuletzt abgerufen am 03.07.2018.

[4] S. Ahava. Troubleshooting cross-domain tracking in google analytics. 2016. URL https://www.simoahava.com/analytics/troubleshooting-cross-domain-tracking-in-google-analytics/. Zuletzt abgerufen am 03.07.2018.

[5] A. Aladeokin, P. Zavarsky, and N. Memon. Analysis and compliance evaluation of cookies-setting websites with privacy protection laws. *IEEE Xplore*, 2017. URL https://ieeexplore.ieee.org/document/8244646/. Zuletzt abgerufen am 03.07.2018.

[6] B. Bruenen. Datenschutzgrundverordnung: Endet die aera der social media plugins? 2017. URL https://www.it-recht-kanzlei.de/social-plugins-datenschutzgrundverordnung-dsgvo.html. Zuletzt abgerufen am 03.07.2018.

[7] A. Christl. *Datenschutz im Internet: Cookies, Web-Logs, Location Based Services, eMail, Webbugs, Spyware* -. disserta Verlag, Hamburg, 2014. ISBN 978-3-954-25646-4.

[8] P. Fleischer. Cookies: expiring sooner to improve privacy. 2007. URL https://googleblog.blogspot.com/2007/07/cookies-expiring-sooner-to-improve.html. Zuletzt abgerufen am 03.07.2018.

[9] J. Geary. Doubleclick (google): What is it and what does it do? 2012. URL `https://www.theguardian.com/technology/2012/apr/23/doubleclick-tracking-trackers-cookies-web-monitoring`. Zuletzt abgerufen am 03.07.2018.

[10] R. Gomer, R. E. Mendes, N. Milic-Frayling, and M. Schraefel. Network analysis of third party tracking: User exposure to tracking cookies through search. *IEEE Xplore*, 2013. URL `https://ieeexplore.ieee.org/document/6690064/`. Zuletzt abgerufen am 03.07.2018.

[11] A. Guenes, B. Van Alsenoy, F. Piessens, C. Diaz, and B. Preneel. Facebook tracking through social plug-ins. 2015. URL `https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf`. Zuletzt abgerufen am 03.07.2018.

[12] S. Hill. Are cookies crumbling our privacy? we asked an expert to find out. 2015. URL `https://www.digitaltrends.com/computing/history-of-cookies-and-effect-on-privacy/`. Zuletzt abgerufen am 03.07.2018.

[13] F. Roesner, T. Kohno, and D. Wetherall. Detecting and defending against third-party tracking on the web. *ACM Digital Library*, 2012. URL `https://dl.acm.org/citation.cfm?id=2228315`. Zuletzt abgerufen am 03.07.2018.

[14] M. Zawadzinski. Why cookie alternatives are vital for the future of mobile advertising. 2015. URL `https://clearcode.cc/blog/cookie-alternative-future-mobile-advertising/`. Zuletzt abgerufen am 03.07.2018.