Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Stefanie Hinck

Entwicklung eines Konzepts zum Monitoring von Cookies und anderen Trackern von Webseiten

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Stefanie Hinck

Entwicklung eines Konzepts zum Monitoring von Cookies und anderen Trackern von Webseiten

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung
im Studiengang Wirtschaftsinformatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Rüdiger Weißbach
Zweitgutachter: Prof. Dr. Ulrike Steffens

Abgegeben am 03.12.2015

Stefanie Hinck

Thema der Bachelorarbeit
Entwicklung eines Konzepts zum Monitoring von Cookies und anderen Trackern von Webseiten

Stichworte
Cookies, Tracking, Online-Werbung, Überwachung

Kurzzusammenfassung
Die vorliegende Arbeit beschäftigt sich mit der Erstellung eines Konzepts zum Monitoring von Cookies und anderen Trackern auf Webseiten. Für die Ausarbeitung werden die Grundlagen des Themenbereichs ermittelt, sowie die datenschutzrechtlichen Aspekte aufgeführt. Die daraus entwickelte Strategie bildet die Grundlage für die empfohlene Realisierung einer Monitoring-Anwendung.

Stefanie Hinck

Title of the paper
Development of a concept for monitoring of cookies and other trackers on websites

Keywords
Cookies, Tracking, Online Advertising, Monitoring

Abstract
The present work deals with the development of a concept for monitoring of cookies and other trackers on websites. For the elaboration the basics of the subject area are determined, and the data protection aspects are listed. The developed strategy forms the basis for the recommended implementation of a monitoring tool.

Inhaltsverzeichnis

Abkürzungsverzeichnis

BDSG	Bundesdatenschutzgesetz
CSS	Cascading Style Sheets
DOM	Document Object Model
EDSB	Europäischer Datenschutzbeauftragter
EU	Europäische Union
FSO	Flash Shared Object
GUI	Graphical User Interface
HbbTV	Hybrid Broadcast Broadband TV
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICC UK	International Chamber of Commerce United Kingdom
ICO	Information Commissioner's Office
JSON	JavaScript Object Notation
KMU	Klein- und Mittelständische Unternehmen
LSO	Local Shared Object
OBA	Online Behavioral Advertising
TMG	Telemediengesetz
UDID	Unique Device Identifier
URL	Uniform Resource Locator

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Tracking – ein Begriff der in der heutigen Zeit bezüglich der Internet-Nutzung nicht mehr weg zu denken ist. Der Nutzer wird „verfolgt“, seine Webseitenaufrufe gespeichert und Profile über ihn erstellt. Datenkraken wie zum Beispiel Google eine ist, speichern dabei nicht nur jede Suchanfrage des Nutzers, sondern ermöglichen es Diensten, außerhalb den Google-eigenen, durch technische Tricks es ihnen gleich zu tun. Einer dieser Tricks, und dabei der wohl bekannteste, ist das kleine „verräterische“ Cookie. Es erlaubt Dritten die Ansammlung und Abspeicherung von Informationen auf dem Rechner des Benutzers. So können über Jahre hinweg alle Suchanfragen und Seitenaufrufe in ein erstelltes Profil gespeist werden, worüber sich der Nutzer letztendlich eindeutig identifizieren lässt (vgl. [MAND11]). Zugleich nimmt aber die Bedeutung des Cookies, aufgrund von sinkender Akzeptanz der Nutzer und den gesetzlichen Änderungen hinsichtlich ihres Handlings, als zentrales Element der Trackingtechnologien im Internet stetig ab. Daraus ergeben sich Marktlücken für Alternativen zum Browsercookie und diese geraten zunehmend in den Fokus der Aufmerksamkeit. Hier sind Verfahren und Technologien aufstrebend, welche die Verwendung von Cookies ergänzen oder sogar überflüssig machen, was keinerseits bedeutet, dass sie nicht weniger in der datenschutzrechtlichen Grauzone stecken.

Benutzer sollten sich deshalb im Klaren sein, welche Informationen sie online über sich preisgeben. Ein wenig auf Facebook aus dem heimischen Nähkästchen plaudern, auf Instagram posten was und wo es Mittag gab - macht doch nichts, es wissen doch nur ein paar Eingeweihte, wer der Autor ist. Was macht es da schon, dass Google jeder Datei ein Schlagwort zuordnet. Ist doch ein praktischer Service, oder nicht?

In Zeiten, in denen vermeintliche YouTube-Stars über ihre intimen Interessen erzählen, mag es altmodisch erscheinen, im Internet auf den Schutz der Privatsphäre zu achten. Es gilt sich immer bewusst zu sein, dass Netzinhalte auch in vielen Jahren noch auffindbar sein können. Denn das Internet vergisst nie.

Im Sinne einer Marktaufklärung wird häufig versucht über die aktuellen technischen Entwicklungen im Bereich Profilbildung und Tracking zu informieren, sowie einen Überblick über die rechtliche Einordnung von Cookies und dazu alternativen Technologien darzulegen. Allen Marktteilnehmern, den Nutzern und den Webseitenbetreibern, soll aufgezeigt werden wie verschiedenste Tracking-Technologien eingesetzt werden können (vgl. [BAUE15]).

1.1 Ziel der Arbeit

Das Ziel dieser Arbeit ist die Entwicklung eines Monitoring-Konzepts zur Überwachung von Cookies und anderen ausgewählten Trackern auf Webseiten, die in Bezug auf die Nutzerverfolgung eingesetzt werden. Dabei ist die erste Aufgabe eine Analyse der bestehenden Technologien, um eine passende Klassifizierung für Cookies und andere Tracker zu finden, welche anschließend auf benutzerfreundliche Weise dargestellt wird. Mit Hilfe der Klassifizierung kann nachfolgend als zweite Aufgabe ein Konzept erstellt werden, welches wiederum als Grundlage für die Softwareentwicklung dienen kann.

1.2 Themenabgrenzung

Das Thema rund um Cookies und anderer Tracker für Webseiten und ihre datenschutzrechtliche Relevanz ist ein breitgefächertes Feld. In dieser Arbeit soll es nicht um die technische Unterscheidung der verschiedenen Tracker, sowie deren unterschiedlichen Standards gehen. Außerdem ist die Datensicherheit für das nach dem Konzept zu erstellende Monitoring-Anwendung zu vernachlässigen, da es nicht um das Anwendung an sich geht. Es wird keine Software entwickelt und daher

werden keine detaillierten technischen Anforderungen wie Ausstattung des Entwickler- und Zielrechners, Prüfeinrichtungen, Zugriffsrechte oder Ähnliches beschrieben.

1.3 Struktur der Arbeit

Die Arbeit ist in vier Kapitel gegliedert, die aufeinander aufbauend eine tiefergehende Spezialisierung der Themen aus den vorangegangen Kapiteln vornehmen. Nach dieser Einführung im ersten Kapitel werden im zweiten Kapitel grundlegende Eigenschaften von Cookies und anderen Trackern im World Wide Web vorgestellt, die für eine personalisierte Nutzerverfolgung maßgeblich sind.
Dabei geht es darum, wie Benutzer mit Webseiten interagieren, wie ihre Interaktionen in Protokollen festgehalten werden und wie der Datenschutz im Internet behandelt wird. Im dritten Kapitel wird nach der Darstellung der Ausgangslage eine Strategie erarbeitet, mit deren Hilfe ein Konzept erstellt werden kann, um zu erläutern, wie ein erfolgreiches Monitoring der verschiedenen Tracker zu gewährleisten ist. Dazu wird zunächst der generelle Aufbau eines Konzepts beschrieben und anschließend wird diesem roten Faden gefolgt. Im vierten Kapitel wird abschließend der Inhalt, aufbauend auf den gewonnenen Erkenntnissen der Arbeit und ihrer Ergebnisse zusammengefasst und ein Ausblick gegeben, an welchen Stellen Weiterentwicklungen vorgenommen werden könnten.

2 Grundlagen

In diesem Kapitel werden die Grundlagen und Hintergründe für die vorliegende Arbeit erläutert. Zunächst wird der Begriff des Cookies, sowie dessen Arbeitsweise und seine verschiedenen Arten beschrieben. Außerdem wird der Frage nachgegangen wie und wonach Cookies klassifiziert werden können (2.1). Im nächsten Abschnitt werden andere Arten von Trackern vorgestellt (2.2). Anschließend wird ein kurzer Überblick über die rechtliche Einordnung von Cookies und dazu alternativen Technologien vorgestellt (2.3).

2.1 Was sind Cookies?

Browsercookies (im Weiteren „Cookies“) stammen aus der Technik der Web-Programmierung, genauer aus der Technik des Hypertext-Transfer-Protokolls (HTTP). Sie dienen zur Speicherung von Information auf dem Webclient. Der Webserver legt Informationen, meist in Textform, dauerhaft (persistent) auf dem Client (Endgerät des Netzwerks) ab, um etwa beim nächsten Besuch der Seite wieder darauf zuzugreifen. Durch Cookies wird eine Wiedererkennung des Nutzers ermöglicht, wobei häufig Benutzerinformationen gespeichert werden. Bei Webseiten die in mehrere Sprachen zur Verfügung stehen, kann die ausgewählte Sprache auf dem Client, durch einen Cookie, hinterlegt werden und beim nächsten Aufruf der Seite wird diese dann direkt in der zuvor gewählten Sprache angezeigt. Ein anderes bekanntes Beispiel für den Einsatz von Cookies liefert die Internetseite www.amazon.de. Geht der Nutzer auf dieser Webseite auf die Suche nach einem Artikel, bekommt er bei einem späteren Besuch diesen und ähnliche Artikel gleich auf der Startseite angeboten. Der Dienstanbieter kann über das Cookie den vorherigen Besuch nachvollziehen und darauf geschickt reagieren (vgl. [WALT08]).

Ebenfalls können die Information gerätespezifisch, gespeichert werden. In dem Cookie wird dann zum Beispiel hinterlegt ob die Webseite über ein mobiles Device aufgerufen wird. Webseiten sind zustandslos, das bedeutet, dass sie keine Zustandsinformation speichern können. Jede Anfrage an den Browser ist in sich abgeschlossen und beinhaltet alle notwendigen Informationen über den Anwendungszustand, da kein Zusammenhang zwischen den einzelnen Anfragen hergestellt werden kann. Hier kommt der Cookie zum Einsatz und übernimmt die Erinnerung in Form von Speicherung. Bei dem wohl populärsten Netzwerkprotokoll HTTP kann das Mitführen von Sitzungsdaten erst auf der Anwendungsebene implementiert werden. Zum Beispiel durch die Übermittlung einer Session-ID im Laufe der Anfrage innerhalb der Request-URL oder dem „Cookie“-Header (vgl. [BEWE14]).

Cookies erlauben dem User sich auf einer Webseite einzuloggen, nebenbei andere Webseiten zu öffnen, und dabei auf der ersten Seite eingeloggt zu bleiben. Sie speichern die Vorlieben, um diese beim Wiederkehren direkt anzuzeigen. Mit jeder übermittelten Datei können Browsercookies übertragen werden, auch mit Bilddateien wie zum Beispiel Werbebannern oder jedem anderen Dateityp. Cookies werden auch verwendet um Webseiten zu beobachten, welche zwischen der eigentlichen Suchanfrage aufgerufen werden. Dadurch können Werbetreibende sich ein Bild der Interessen des Users zusammenstellen. Wenn der Anwender dann eine Seite besucht, die Werbung des Werbetreibenden ausspielt, können sie diese in das Interessenfeld des Users mit aufnehmen. Das nennt man Verhaltensorientierte Werbung. So gut wie alle Webseiten nutzen Cookies auf die ein oder andere Weise und jede Seite die besucht wird, speichert Cookies auf der Festplatte des Anwenders, um diese später wieder abzurufen.
Cookies sind nützlich - sie erlauben modernen Webseiten, auf die Art zu arbeiten, wie die Menschen sie zu schätzen gelernt haben - mit zunehmender Personalisierung und interaktiven Funktionen. Wie dem auch sei können Cookies ebenfalls dazu benutzt werden das Web-Erlebnis des Users auf unerwartete und missfallende Weise zu manipulieren. Dies kann zwar zum eigenen Vorteil, aber immer öfter zum Vorteil Dritter geschehen. Es ist nahezu unmöglich durch reines Ansehen der Cookies festzustellen wer denn nun den Vorteil hat. Der Anwender muss sich auf die Angaben der Webseite verlassen, die er besucht, wie diese die

Cookies verwenden (vgl. [GOVE14]). Welche Cookies im Browser gespeichert sind, lässt sich über die Datenschutzeinstellungen im Browser herausfinden.

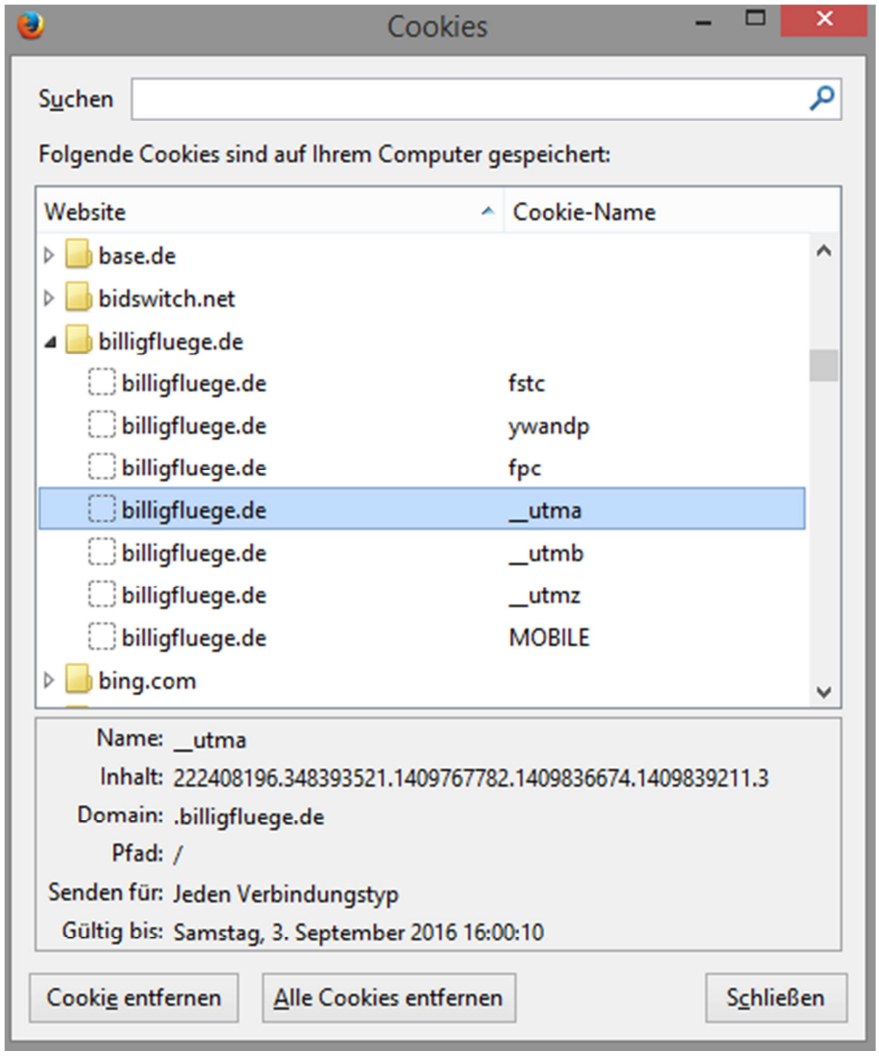

Abbildung 1: Cookie-Verwaltung mit dem Mozilla Firefox

2.1.1 Arbeitsweise und Datenstruktur von Cookies

Cookies stammen aus der Technik des HTTP-Protokolls (siehe 2.1). Sie werden im HTTP-Header gesetzt, nach dem die Anweisung SET-Cookie aufgerufen wurde. Abbildung 2.1 zeigt den Anfang einer cURl-Anfrage an die Seite www.chefkoch.de; dabei ist zu sehen, wie der Webserver einen Cookie setzt.

```
* Trying 185.13.208.22...
* Connected to www.chefkoch.de (185.13.208.22) port 80 (#0)

> GET / HTTP/1.1
> User-Agent: curl/7.26.0
> Host: www.chefkoch.de
> Accept: */*

< HTTP/1.1 200 OK
< Server: nginx
< Content-Type: text/html; charset=utf-8
< Vary: Accept-Encoding, User-Agent
< Last-Modified: Wed, 29 Jul 2015 14:05:21 GMT
< Set-Cookie: ckSession=es1vn1ulv2ara124qahnmsi5h5; path=/; HttpOnly
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Pragma: no-cache
< X-Frame-Options: SAMEORIGIN
< Content-Security-Policy: frame-ancestors 'self'
< X-Content-Type-Options: nosniff
< Cache-Control: must-revalidate, no-cache, no-store, post-check=0, pre-check=0, private, no-transform
< Content-Length: 133966
< Accept-Ranges: bytes
< Date: Wed, 29 Jul 2015 14:05:29 GMT
< X-Varnish: 2173978605
< Via: 1.1 varnish
< Connection: keep-alive
< age: 0
```

Abbildung 2: Setzen von Cookies im HTTP-Header von www.chefkoch.de

Die Cookie-Informationen, welche mit Hilfe dieser HTTP-Methode vom Server zum Client übertragen werden, werden anschließend vom Client in Text-Dateien abgelegt. Diese sind wiederum durch einen einfachen Editor veränderbar.

Zur Datenstruktur lässt sich sagen, dass die Speicherung eines Key-Value-Paares den Kern eines Cookies bildet. Ein „Schlüssel-Wert-Paar“ stellt zwei miteinander verbundene Datenelemente dar. Zusammengesetzt ist es aus einer eindeutigen Kennung für bestimmte Daten und dem Wert, welcher entweder die identifizierten Daten oder einen Zeiger auf den Speicherort dieser Daten beinhaltet. Neben diesen Informationen gehören noch zahlreiche weitere Werte zu einem Cookie.

Die nachfolgende Tabelle 2.1 zeigt welche anderen Attribute für Cookies bereit stehen.

Attribut	Bedeutung
`key=value`	die Kerninformation des Cookies: Name und Wert, mit „=“ getrennt
`version`	Information für das Cookie-Management (Dezimalzahl)
`expires`	Gültigkeit des Cookies (Zeitpunkt der automatischen Löschung in UTC)
`max-age`	Ablaufzeit in Sekunden
`domain`	Domain oder Bestandteil des Domainnamens, für den das Cookie gilt
`path`	Pfad-Angabe, um die Gültigkeit des Cookies auf einen bestimmten Pfad zu beschränken
`port`	Beschränkung des Ports
`comment`	Kommentar zur Beschreibung des Cookies
`commenturl`	URL-Angabe für die weitere Beschreibung des Cookies
`secure`	erzwingt die Rücksendung des Cookie über eine mindestens ebenso sichere Verbindung, faktisch in https
`discard`	erzwingt Löschung des Cookies bei Beendigung des User-Agents

Tabelle 1: Cookie-Attribute in http 1.1 (vgl. [WALT08])

2.1.2 Arten von Cookies

Es gibt viele unterschiedliche Arten von Cookies, aber es gibt auch verschiedene Arten sie einzuordnen. Im Folgenden werden die populärsten Cookie-Arten vorgestellt. Die ersten sechs Arten beziehen sich dabei auf die ‚normalen‘ Text-Cookies (vgl. [GOVE14]). Abschließend wird die relative neue junge Art der Flash-Cookies vorgestellt.

First-Party-Cookies

Ein Schlüsselattribut von Cookies ist ihr Anbieter. Wird ein Browsercookie, von der Domain der Webseite, auf der sich ein Internetnutzer gerade wissentlich aufhält, gesetzt, handelt es sich um einen First-Party-Cookie (vgl. [BAUE15]). Nur der Anbieter der Domain kann die Inhalte abrufen und lesen, nachdem der Cookie gesetzt wurde. First-Party-Cookies werden nur gesetzt, wenn der Internet-Nutzer eine Webseite besucht. So können diese Cookies üblicherweise nicht zum Verfolgen

der Aktivitäten verwendet werden oder Daten zwischen Seiten austauschen. Der Eigentümer der besuchten Seite kann trotzdem Daten durch diese Cookies sammeln und diese Informationen nutzen, um die Webseite für den Anwender interessanter zu gestalten. Die gesammelten Daten können jedoch ungeachtet dessen außerhalb der Webseite verwendet oder sogar an andere Organisation verkauft werden. Falls dies im Interesse des Eigentümers geschieht, muss dies in der Datenschutzerklärung der Webseite aufgeführt und erklärt werden. Viele Desktop Browser erlauben dem Anwender eine Liste der gesetzten Cookies einzusehen und meist werden die Cookies der Anbieter-Domain nach sortiert angezeigt (vgl. 2.1.1).

Third-Party-Cookies

Ist der Anbieter eines Cookies ein anderer, als der in der Browser-Adressleiste angezeigte, zum Zeitpunkt seines Herunterladens, handelt es sich um einen sogenannten „Third-Party-Cookie“ - einen Cookie, gesetzt von einem Drittanbieter. Diese Cookies werden üblicherweise auf Webseiten via Skript oder Markierung gesetzt. Manchmal enthalten Skripte zusätzliche Funktionen für die Seite, wie das Einfügen eines Inhaltes, der auf sozialen Netzwerkplattformen geteilt werden kann. Zum Beispiel enthält eine vom Anwender besuchte Seite ein Video des Dienstes YouTube. Dieses Video wurde vom Eigentümer der Seite eingebaut, unter der Verwendung von Code, welcher durch YouTube zur Verfügung gestellt wurde. YouTube ist somit durch dieses Code-Fragment in der Lage Cookies zu setzten. Es kann erkannt werden, ob das Video angeschaut, oder die Webseite mit dem enthaltenen Video einfach nur besucht wurde. Die Verbindungen zum Austausch von Third-Party-Cookies wird typischerweise nicht von den Benutzern wahrgenommen.
Online Werbung ist die gebräuchlichste, verbreitete Anwendung von Cookies durch Drittanbieter. Third-Party-Cookies bieten geeignete Rahmenbedingungen, um bei vielen Benutzern mit geringem Aufwand sehr effektives Tracking betreiben zu können (vgl. [SCHN14]). Durch das Hinzufügen einer Markierung, welche Werbung anzeigen kann, können Werbetreibende die Anwender (oder ihre Geräte) über mehrere Webseiten hinweg verfolgen. Dies ermöglicht es ihnen, ein nutzungsbasiertes Profil des Anwenders zu erstellen und ihn anschließend mit, auf seine Interessen zugeschnittene, Werbung zu bedienen. Der Nutzen von

Drittanbieter-Cookies wird häufig als aufdringlich und als Verletzung der Privatsphäre gesehen. Aktivitäten wie diese, sind ein großer Antrieb für die Entwicklung neuer Gesetze im Datenschutz, gerade auch für die sogenannte „Cookie-Richtlinie“ der Europäischen Union (offizieller Name: E-Privacy-Richtlinie 2009/136/EG).

First- und Third-Party-Cookies zeigen technisch und in den Nutzungsmöglichkeiten so gut wie keine Unterschiede auf. In den Datenschutzeinstellungen des Browsers kann der Nutzer aber über den Umgang mit den beiden Typen des Browsercookies entscheiden (vgl. [BAUE15]).

Session-Cookies

Session-Cookies sind nur temporär im Speicher des Browsers hinterlegt und werden gelöscht, sobald der Browser geschlossen wird. Allerdings überleben sie das Navigieren über verschiedene Webseiten. Muss der Anwender sich jedes Mal auf einer Webseite einloggen wenn er den Browser öffnet und diese Seite aufruft, dann wird ein Session-Cookie genutzt, um die Anmeldedaten zu speichern. Viele Webseiten benutzen diese Art von Cookies für wesentliche Funktionen und um sicherzustellen, dass die Seiten so schnell und effizient wie möglich an den Browser gesendet werden.

Persistent-Cookies

Wie der Name schon vermuten lässt, wird diese Art des Cookies auf dem Computer des Anwenders gespeichert und kann nach Herunterfahren und anschließendem Neustart immer noch vorhanden sein. Persistent-Cookies wird bei der Erzeugung ein Ablaufdatum mitgegeben. Wird kein Datum übergeben, ist der erzeugte Cookie automatisch ein Session-Cookie. Das Ablaufdatum wird normalerweise als die Zeit gesetzt, an welcher der Cookie zum ersten Mal erzeugt wird, plus eine Anzahl an Sekunden, die vom Programmierer selbst festgelegt wird. Ein „richtiges“ Limit für das Ablaufdatum ist nicht vorgegeben. Somit kann es auch für 20 Jahre in der Zukunft gesetzt sein. Zusätzlich dazu kann bei erneutem Besuch der Webseite, die

den Cookie gesetzt hat, ein automatisches Update des Cookies erfolgen und dadurch auch eine Überarbeitung des Ablaufdatums stattfinden.
Meldet sich der User auf einer Webseite an, fährt seinen Computer herunter, startet ihn neu, besucht die gleiche Webseite und ist immer noch angemeldet, dann handelt es sich um den Gebrauch eines Persistent-Cookies.
Diese Art von Cookie wird auch benutzt, um Nutzer zu tracken. Die dann gesammelten Daten werden zur Untersuchung der Interessen der Nutzer verwendet. Diese Methode ist als Web Analyse bekannt. Seitdem Google seine eigene, frei nutzbare, Analyse-Technologie auf den Markt gebracht hat, verwenden nahezu alle Webseiten eine Form der Web Analyse. Allerdings rivalisieren auch kostenpflichtige Dienste mit Google. Analytische Cookies sind heutzutage die wohl üblichste Form der Persistent-Cookies. Sonderbarerweise können einige Persistent-Cookies eine kürzere Lebensdauer, als manche Session-Cookies haben.
Erstgenannte können programmiert werden, um innerhalb von wenigen Sekunden wieder zerstört zu werden, wohingegen die Session-Cookies immer bis zum Schließen des Browsers existieren.

Secure-Cookies

Secure-Cookies, welches übersetzt „Sichere Cookies“ bedeutet, werden nur über das sichere Hypertext-Übertragungsprotokoll (HTTPS) übertragen. Dies wird typischerweise auf den Einkaufsseiten von Onlineshopping-Seiten verwendet. Dadurch wird sichergestellt, dass jegliche Informationen in dem Cookie verschlüsselt sind, während er zwischen Webseite und Browser weitergeleitet wird. Auch Cookies die nicht im E-Commerce verwendet werden, wie zum Beispiel um Kreditkarteninformationen zu speichern, können Secure-Cookies sein.

HTTP-Only Cookies

Wenn ein Cookie ein HTTP-Only-Attribut gesetzt bekommen hat, verhindert der Browser jedem Clientskript (wie Java-Skript) den Zugriff auf den Inhalt des Cookies.
Dies schützt vor sogenannten webseitenübergreifenden Scripting- (XSS) Angriffen, bei denen ein schädliches Skript versucht, den Inhalt eines Cookies an eine dritte Webseite zu senden.

Flash Cookies

Flash-Cookies (oder Local Shared Object, kurz LSO) sind eine neue Art der Datensammler. Sie haben in der Regel die Dateiendung „.sol“ (vgl. [SCHO12]). Flash-Cookies sind an den Adobe Flash-Player gebunden, welcher von der ehemals Macromedia GmbH, jetzt übernommen von Adobe Systems, bereitgestellt wird und als Standardprogramm zur Wiedergabe von Animationen und Filmen im Netz gilt. Diese Cookies werden erzeugt beim Aufrufen von Flash-Inhalten (Filme, Werbung, Streaming Media, etc.) über einen Browser. Ähnlich wie beim Browser-Cookie werden ebenfalls einzelne Textdateien pro Domain angelegt (vgl. [BAUE15]). Wie die vorher beschriebenen Arten von Cookies, können auch Flash-Cookies Informationen über Surfgewohnheiten der Anwender speichern und tragen so zur Erstellung von Nutzungsprofilen bei (vgl. [KRUE07]). Im Gegensatz zum Umfang des HTTP-Cookies, welcher auf vier Kilobyte beschränkt ist, erlauben Flash-Cookies die Speicherung von bis zu 100 Kilobyte. Die gespeicherten Daten liegen ohne Verfallsdatum auf dem Rechner des Anwenders (Client) und werden über den Browser an den Zentralrechner (Host) gesendet. Die Daten bleiben für die Wiedererkennung solange gespeichert und verwendbar, bis ein Benutzer sie eigenhändig löscht. Nicht alle Browser verfügen in ihren Datenschutzeinstellungen über die Möglichkeit zusätzlich Flash-Cookies zu verwalten, abzulehnen oder zu löschen. Infolgedessen muss der Benutzer auf zusätzliche installierte Browser-Plug-Ins oder eigene Managementkomponenten des Flash-Players in der Systemsteuerung zurückgreifen (vgl. [SCHN14]).
Des Weiteren können diese Cookies mit den klassischen Cookies interagieren. Dabei werden diese vom Flash-Cookie kopiert, aufbewahrt und können beim nächsten Besuch einer Webseite wiederhergestellt werden, auch wenn der klassische Cookie vorher vom Anwender gelöscht wurde. Das wird als „respawning“, welches übersetzt „erneut starten“ bedeutet, bezeichnet (vgl. [KRAS10]). YouTube zum Beispiel nutzte bis vor einem halben Jahr Flash Cookies, um die vom Nutzer eingestellte Video-Lautstärke zu speichern. Nach der Umstellung auf HTML5 kommt dieses spezielle Cookie bei der Video-Plattform allerdings nicht mehr zum Einsatz. Auch Werbetreibenden ist nun nicht mehr gestattet Flash-Cookies für ihre Anzeigen zu verwenden (vgl. [GOOG15a]).

Die praktische Bedeutung von Flash-Cookies als alternative Trackingtechnologie ist allerdings tendenziell abnehmend. Adobe Flash wird nicht mehr von allen reichweitenstarken Betriebssystemen unterstützt und verliert daher allmählich seine Rolle als universelle technologische Plattform für bewegte Bildinhalte im Internet (vgl. [BAUE15]).

2.1.3 Wie und wonach können Cookies klassifiziert werden?

Im Einklang mit den jüngsten Änderungen der europäischen Rechtsvorschriften verlangt das britische Gesetz neuerdings von Webseitenbetreiber die Erlaubnis der Webseitenbenutzer einzuholen, wenn bestimmte Arten von Cookies auf ihren Geräten gesetzt werden. Dies erhöht die Pflicht auf den Webseiten sicherzustellen, dass die Besucher verstehen, was Cookies sind und warum die Webseitenbetreiber und andere Dritte sie benutzen wollen.
Aufgrund dieser Gesetzeslage hat die Internationale Handelskammer UK (ICC UK) im April 2012 einen Katalog mit Richtlinien veröffentlicht, in denen sie beschreibt wie und wonach Cookies klassifiziert werden können (vgl. [ICCU12]).

Kategorie 1 – Strictly Necessary Cookies

Die Cookies der ersten Kategorie, die durch die ICC festgelegt wurde, beschreiben Cookies die streng erforderlich sind. Diese Cookies sind notwendig, damit der User sich auf der angebotenen Webseite bewegen und dessen Funktionen, wie Zugang zu gesicherten Bereichen der Seite, nutzen kann. Ohne den Service dieser Cookies könnten Warenkörbe nicht zusammengestellt oder Online-Bezahlungen nicht geleistet werden. Ein weiteres Beispiel ist das Speichern von vorangegangenen Aktionen, wie den Status des Anwenders, seine Texteingaben oder Spracheinstellungen. Nach Ansicht der Datenschutzbeauftragen des Vereinigten Königreichs (Information Commissioner's Office – ICO) kann nur eine geringe Menge der Aktivitäten im Netz als „streng erforderlich“ kategorisiert werden. Der Nutzen dieser Cookies muss als ein Service auf der Webseite zur Verfügung gestellt sein, welcher explizit vom Benutzer angefordert wurde.

Kategorie 2 – Performance Cookies

Die Cookies der zweiten Kategorie „Verhalten" sammeln Information darüber, wie der Besucher die Webseite nutzt. Zum Beispiel welche Unterseiten er am häufigsten besucht und ob er Fehlernachrichten dieser Webseiten erhält. Es werden keine Informationen gesammelt, die den Nutzer identifizieren könnten. Daher sind alle Daten, die in den Verhaltensorientierten-Cookies gespeichert werden aggregiert und dadurch anonymisiert. Sie werden ausschließlich für die Verbesserung des Wissens über die Arbeitsweise der Webseite verwendet. In diese Kategorie fallen Cookies die zur Web-Analyse genutzt werden. Weitere Beispiele sind Cookies, welche die „response rate (click-through rate)", was übersetzt Antwortrate bedeutet, speichern. Diese verbessern die Wirksamkeit von Werbung, die auf einer Webseite außerhalb der Ziel-Webseite erworben wurde. Des Weiteren fallen Cookies, die für das Affiliate-Tracking eingesetzt werden, in die zweite Kategorie. Diese werden genutzt, um Partner („affiliates") zu informieren, wenn ein Besucher einer Webseite später eine Partnerseite der Ausgangsseite besucht hat. Neben diesen gibt es außerdem Cookies für das Fehler-Management. Hier werden die Fehler auf einer Webseite gemessen, welches in der Regel die Serviceverbesserung oder das Beschwerdemanagement unterstützen soll.

Kategorie 3 – Functionality Cookies

In der dritten Kategorie „Funktionalität" werden Cookies zusammengefasst, welche der Webseite erlauben Eingaben wie Benutzername, Sprache oder Region zu speichern, um erweiterte, personalisierte Funktionen zu bieten. Angenommen eine Webseite ist in der Lage lokale Wetterberichte oder Verkehrsnachrichten bereitzustellen, dann ist in einem Cookie die Region, in der sich der Anwender gerade befindet, hinterlegt. Diese Cookies werden außerdem genutzt, um Änderungen der Einstellungen, wie zum Beispiel die Größe oder Art der Schrift, oder ähnliche, individuell anpassbare, Bereiche der Webseite, zu speichern. Die Informationen die diese Cookies sammeln können anonymisiert sein und nicht dazu verwendet werden die Internet-Aktivitäten zu verfolgen. Kategorie-3-Cookies werden auch eingesetzt, um auszuschließen, dass einem Anwender der gleiche Service ein weiteres Mal angeboten wird, welchen er im Vorfeld verweigert hat.

Zusammengefasst speichern die Cookies verschiedene Einstellungen, um das Anwendererlebnis zu verbessern.

Kategorie 4 – Targeting or Advertising Cookies

Die vierte Kategorie beschreibt Cookies mit einer Zielausrichtung, wie beispielsweise Werbezwecke. Sie werden eingesetzt um dem Anwender seinen Interessen nach relevante Anzeigen zu liefern. Sie werden zum einen verwendet, um die Anzahl zu limitieren, wie oft die Anzeige vom User gesehen werden soll. Zum anderen helfen sie die Effektivität von Werbekampagnen zu steigern. Normalerweise werden diese Cookies mit Erlaubnis des Webseitenbetreibers von den Werbetreibern direkt gesetzt. Sie speichern die vom Anwender besuchte Webseite und teilen diese Information anschließend mit anderen Organisatoren, wie Werbetreibenden. Häufig sind Cookies mit Zielausrichtung oder Werbezweck mit der Funktionalität der Webseite verknüpft, welche von einer anderen Organisation zur Verfügung gestellt wird. Die Cookies der vierten Kategorie sammeln Informationen über das Verhalten des Nutzers, um diesen ihren Interessen nach relevante Werbung auszuspielen.
Meist werden diese Cookes von Drittanbietern gesetzt. Sie sind immer persistent, haben aber ein zeitliches Limit. Sie enthalten einen individuellen Schlüssel, der in der Lage ist das anwenderspezifische Verhalten zu speichern (vgl. [ICCU12]).

2.2 Andere Methoden des Trackings

Web-Tracking bezeichnet im Allgemeinen die Aufzeichnung und Auswertung des User-Verhaltens im Internet. Es gilt, dass Surfverhalten der Anwender auch jenseits eines einzelnen Anbieters nachvollziehen zu können. Dabei ist das Einbinden von fremden Inhalten auf Webseiten der springende Punkt. Neben den klassischen Cookies haben sich im Laufe der Zeit noch andere Technologien entwickelt. In den nachfolgenden Ausführungen werden Server-Logfiles, Pixel-Tracking, zwei Arten des Fingerprintings, Cross-Device-Tracking, Super-Cookies und Mouse-Tracking vorgestellt.

Server Logfiles

Zur Erhebung von Informationen über das Nutzerverhalten von Webbesuchern kommt häufig die Server-Logfile-Analyse zum Einsatz. Hierbei werden beim Zugriff auf einen Web-Server automatisch für jedes aufgerufene Element (HTML-Seiten, Bilder, PDFs, etc.) Einträge in einer Logbuch-ähnlichen Datei erzeugt. Es können der Zeitpunkt des Zugriffs, IP-Adresse des Nutzers und des angefragten Elements, aber auch die zuvor besuchte URL gespeichert werden. Für die Erstellung und spätere Analyse von Logfile-Daten ist in der Regel keine Änderung der Webseite erforderlich, denn die Logfiles werden vom Server automatisch erzeugt. Eine Auswertung der angefallenen Daten kann wiederspiegeln, wie häufig eine PDF-Datei heruntergeladen wurde, oder wie häufig eine Webseite überhaupt aufgerufen wurde. Kostenlose Anwendungen für die Logfile-Analyse stehen außerdem jedem öffentlich zur Verfügung (vgl. [STAH12]).

Pixel Tracking

Eine ähnliche Methode ist das Pixel-Tracking, auch bekannt als der Einsatz von Zählpixeln oder Web-Bugs. Es handelt sich bei den Zählpixeln um Bilder, die von einem Tracker geladen und wie andere Bilder in Embedded-Webseiten (vom deutschen „einbetten“) integriert werden (vgl. [SCHN14]). Diese sind meist 1x1 Pixel groß und werden im Hintergrund geladen, oder verstecken sich in anderen Grafiken (vgl. [ROET99]). Deren Inhalt ist meist farblos bzw. transparent und somit für den

Nutzer nicht erkennbar. Beim Aufrufen einer Webseite, wird also gleichzeitig der Web-Bug von einem speziellen Analyse-Server heruntergeladen. Diese werden wiederum häufig von externen Dritten betrieben. Für die Darstellung einer Webseite haben die Web-Bugs keine Bedeutung. Die Zählpixel sind nur kleine Gehilfen in Bezug auf die Gewinnung von Kennzahlen über Webbesucher (vgl. [STAH12]). Ihr einziger Zweck besteht quasi darin, dass der Browser des Nutzers Kontakt mit dem Tracker aufnimmt. Bei diesem Verfahren wird teilweise eine Kombination mit JavaScript notwendig, um Daten über das genutzte Betriebssystem (was Rückschlüsse auf die Nutzung mobiler Endgeräte zulässt) oder den Browsertyp zu erheben. Des Weiteren kann ein Tracking-Pixel IP-Adressen (ermöglicht Rückschlüsse auf den Internet-Service-Provider und Standort), die URL der besuchten Webseite, die URL des Web-Bug selbst, den Zeitpunkt, an dem der Web-Bug angeschaut wurde, sowie die Informationen eines zuvor gesetzten Cookies an einen Server senden (vgl.[ONPA15a]).

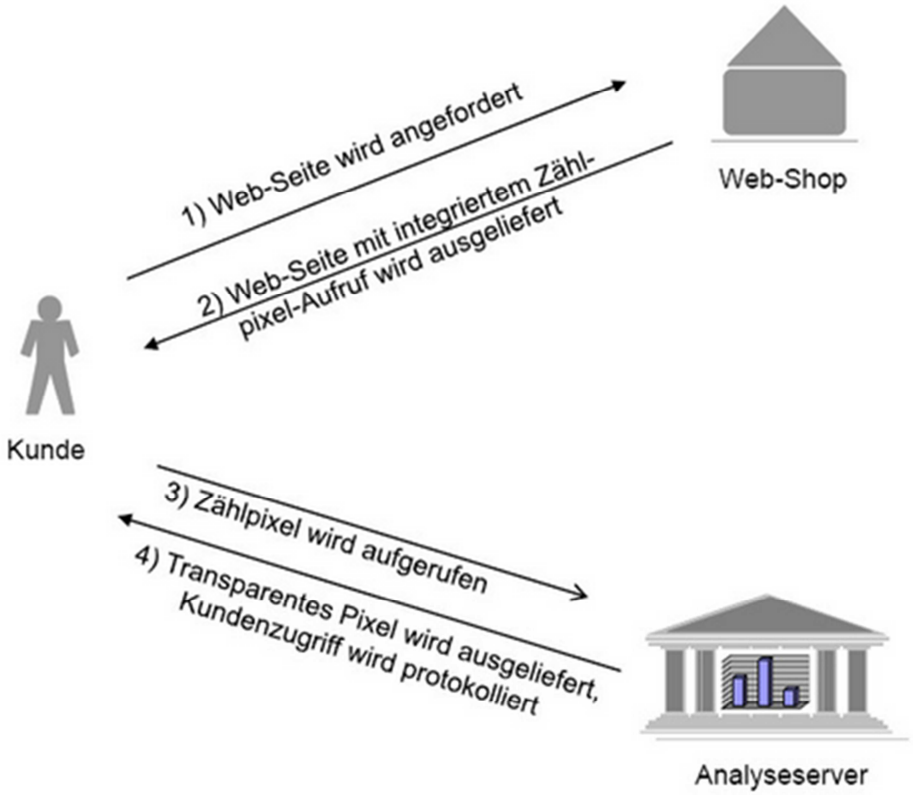

Abbildung 3: Ablauf des Zählpixel-Verfahrens (vgl. [STAH12])

Fingerprinting

Im Kontext von IT-Systemen wird das Fingerprinting als Verfahren bezeichnet, dessen Ziel es ist, ein Gerät anhand einer Kombination von Hard- und Software-Merkmalen wieder zu erkennen. Je mehr Merkmale ermittelt werden können, desto größer ist zwangsläufig die Menge möglicher Kombinationen. Diese Merkmalskombination bildet einen annähernd eindeutigen Schlüssel, denn die Wahrscheinlichkeit für dieselbe Kombination von Merkmalen auf einem zweiten Gerät ist sehr gering. Man unterscheidet zwei Arten von Fingerprinting: Browser- und Canvas-Fingerprinting (vgl. [BAUE15]).

Canvas-Fingerprinting

Canvas ist ein HTML5-Element. Canvas (vom englischen „canvas“ für Leinwand) wird benutzt, um Grafiken oder Animationen auf einer Webseite mittels JavaScript zu zeichnen. Abgesehen davon kann Canvas zusätzlich als ein Maß für die Informationsdichte im Browser-Fingerprinting genutzt werden. Hierbei werden Daten über den Browser und dessen zu Grunde liegendes System in Erfahrung gebracht, wodurch Canvas im Online-Tracking Verwendung findet. Im Gegensatz zu Cookies werden beim Canvas-Fingerprinting die einzigartigen Merkmale des vom User benutzen Gerätes verwendet, um ein Canvas-Bild zu erzeugen. Dieses Bild enthält einen kurzen Text und wird im Hintergrund geladen. Wie das Bild letztendlich aussieht hängt von den individuellen Parametern, wie Betriebssystem, Grafikkarte, Browser, etc., des Users ab. Das Bild wird ohne Kenntnis des Nutzers gerendert (die Webinhalte werden durch den Webbrowser in Bildschirmdarstellung und hier konkret in ein Bild umgesetzt). Es entsteht ein Fingerabdruck. Diesem wird eine ID vom Server zugewiesen und erlaubt es Spuren des Nutzers im Internet zu verfolgen (vgl. [ONPA15]). Die Technik basiert auf dem Fakt, dass das gleiche Canvas-Bild auf verschiedenen Computern unterschiedlich gerendert werden kann. Web-Browser verwenden unterschiedliche Bildverarbeitungssysteme, Bildexportoptionen, Kompressionen, und die fertigen Bilder können unterschiedliche Prüfsummen erhalten, auch wenn sie auf Pixelebene identisch sind. Neben der Bildformat-Ebene, können sie sich auch aufgrund der Systemebene unterscheiden (vgl. [BROW15]). Betriebssysteme haben verschiedene Schriftarten,

verwenden unterschiedliche Algorithmen und Einstellungen für Anti-Aliasing (auch Kantenglättung, zur Verminderung von unerwünschten Effekten durch begrenzte Bildauflösung) und Subpixel-Rendering (engl. Teilbildpunktwiedergabe, zur Verbesserung der Textdarstellung auf Farbbildschirmen).

Browser-Fingerprinting

Browser-Fingerprinting ist eine zunehmend verbreitete, wenn auch noch eher selten diskutierte Technik der Identifizierung durch die einzigartigen Informationsmuster die sichtbar werden, wenn der Nutzer eine Webseite besucht. Die resultierende Liste von Merkmalswerten stellt dabei den „Fingerabdruck" eines Browsers dar und wird anschließend an eine Webseite zur Identifikation des Nutzers übertragen. Die gesammelten Informationen sind recht umfangreich und können den Browsertyp und -version, Betriebssystem, Bildschirmauflösung, unterstützte Schriftarten, Plug-Ins, Zeitzone, Sprachen, Präferenzen und sogar Hardware-Konfigurationen umfassen. Je nach Browser kann es darüber hinaus noch eine Vielzahl weiterer Konfigurationsaspekte geben, die hierbei als Identifikator zu verstehen sind (vgl. (ECKE10]). Wenn der Nutzer eine Webseite besuchen möchte sendet diese Informationen an den Webbrowser, sodass sie angezeigt werden kann. Während der Browser die Webseite lädt, werden auch Anzeigen von einem Online-Ad-Broker geladen. Der Ad-Broker antwortet, indem er Werbeanzeigen zusammen mit einem Skript sendet, welches Informationen über den Browser und den Computer sammelt, um den Nutzer eindeutig zu identifizieren. Anschließend meldet das Fingerprinting-Skript die Informationen an den Ad-Broker zurück, welcher diese wiederum an seinen Fingerprinting-Anbieter weiterleitet. Hier werden die Daten gegen eine Datenbank abgeglichen und an den Ad-Broker wird eine eindeutige Nummer oder ein Code zurückgesandt, um den Nutzer zu identifizieren. Resultierend daraus kann der Ad-Broker diesen Identifikator nutzen, um zu jeder Zeit den Überblick über die Online-Aktivitäten des Nutzers zu erhalten, wenn dieser eine Webseite mit seinen Inseraten besucht (vgl. [NIKI14]).

Cross Device Tracking

Mit der Zeit verändert sich auch das Nutzungsverhalten im Web. Inzwischen verwenden Nutzer mehrere verschiedene Geräte („Cross-Device") um im Internet nach Informationen zu suchen. Dieses Online-Verhalten („Customer Journey") wurde jahrelang durch gesetzte Tracking-Cookies beim Besuch einer Webseite bewältigt. In der heutigen Multi-Device-Welt ist dies jedoch allein nicht mehr ausreichend. Das Cross-Device-Tracking setzt deshalb auf eine eindeutige, persistente User-ID, die geräteübergreifend gesetzt werden muss (vgl. [SCHU14]). Diese Methode wird oft genutzt, wenn User sich eindeutig durch einen Login oder einen Newsletter identifizieren. Ist der User dann mit der ID markiert, wird diese jedes Mal aus der Datenbank der Tracking-Software herausgesucht, sobald er sich zum Beispiel einloggt. Benutzt nun der gleiche User später sein Handy oder Tablet, und ruft die entsprechende Webseite wieder auf, kann er eindeutig zugeordnet werden (vgl. [ONPA15]). Der untenstehende Code zeigt, wie die User-ID mit Hilfe von JavaScript in den Tracking-Code eingebunden wird:

```
ga('create', 'UA-XXXX-Y', 'auto');
ga('set', '&uid', {{ USER_ID }});
ga('send', 'pageview');
```

Es wird eine eigene, einzigartige, anhaltende und nicht-personenbezogene String-ID angeboten, um jeden angemeldeten Benutzer darzustellen (z.B. für die USER_ID „12345"). Diese ID wird meist durch ein Authentifizierungssystem bereitgestellt. Anschließend wird die Benutzer-ID, mittels der zum Anmelden verwendeten ID auf den Tracker gesetzt.

Super-Cookies

Der Begriff „Super-Cookie" ist eine im Netz weit verbreitete Bezeichnung, die allerdings falsche Assoziationen weckt. Es handelt sich hier nicht um eine „verschlimmerte" Art des Browser-Cookies. Diese Art der Speicherung ähnelt den LSO, die tatsächlicher Weise auch als Flash-Cookies bezeichnet werden. Was

der Internet-Nutzer also unter einem Super-Cookie versteht ist das Verfahren der DOM-Storage.

DOM-Storage wird als ein verbesserter Verwaltungsmechanismus in Arbeitsentwürfen der HTML-5-Empfehlung, die Ende 2010 von dem World Wide Web Consortium (W3C) veröffentlicht wurden, vorgeschlagen (vgl. [WORL15]). Dennoch wird es formal erst seit kurzem als Internet-Standard betrachtet. DOM bezieht sich auf den veralteten Begriff „Document Object Model“ und macht daher wenig Sinn als Beschreibung für den Browser-Speicherplatz. Ähnlich wie HTTP-Cookies ist DOM-Storage ein Mechanismus für die Aufrechterhaltung des Zustandes eines Benutzers auf einer bestimmten Website. Es wurde als großes Ablagefach, welches lokal auf dem Rechner des Benutzers liegt, konzipiert. Gegenüber regulären Cookies, bietet der Mechanismus allerdings zwei Vorteile. Zum einen vermeidet der DOM-Mechanismus kritische Wettlaufsituationen, welche bei gleichzeitigen Browser-Sitzungen auftreten können. Zum Beispiel, wenn zwei Browserfenster den Benutzer zu der gleichen Webseite navigieren, können Cookie-Daten, die in jeder Sitzung übertragen werden, überschrieben oder in einer Weise aggregiert werden, die zu unerwartetem Verhalten führt. Zum anderen weist DOM-Storage eine viel größere Kapazität auf. Es erlaubt Megabytes an persistenter Speicherung auf Seiten der Benutzer-Kommunikation und ermöglicht Webseiten Leistungsverbesserungen in Form eines großen Zwischenspeichers. Mit diesen Vergrößerungen hängen aber die gleichen Third-Party-Tracking-Risiken zusammen, wie bei den regulären Browser-Cookies. Zusätzlich erhöht die Sammlung von hochspezifischen Anwenderdaten die Schwere der Eingriffe in die Privatsphäre durch Dritte. Werbetreibende können eindeutige Kennungen - gespeichert in ihren lokalen Speicherbereichen - nutzen, um einen Benutzer über mehrere Sitzungen hinweg zu verfolgen, ein Interessenprofil über ihn aufbauen und somit zielgerichtete Werbung zu ermöglichen. In Verbindung mit einer Webseite, welche die realen Identitäten ihrer Benutzer kennt, (zum Beispiel eine E-Commerce-Website, die authentifizierte Anmeldeinformationen erfordert), könnte dies eine Verfolgung mit größerer Genauigkeit, als in einer Welt mit rein anonymer Web-Nutzung, ermöglichen (vgl. [MITT10]).

Mouse Tracking

Mouse-Tracking, oder auch bekannt als „Cursor-Verfolgung“, wird verwendet, um die Mauszeiger Positionen des Benutzers auf Webseiten zu sammeln. Unter der Verwendung von JavaScript muss keine zusätzliche Software auf dem Computer des Benutzers installiert werden, es muss lediglich JavaScript aktiviert sein, damit die Daten von der Webseite gesammelt werden können. Mouse-Tracking mit Hilfe von JavaScript wird häufig auf High-Traffic-Webseiten, wie Suchmaschinen, eingesetzt. Damit werden Mausbewegungsdaten gesammelt, ohne die Performance des Computers zu beeinflussen (vgl. [HUAN11]).
Viele Maus-Tracking-Anwendungen bieten eine große Anzahl an Daten, wie die Position der Maus (in Bezug auf die Bildschirmkoordinaten beziehungsweise die Koordinaten im Client-Bereich des Browserwindows), einen Zeitstempel, jeden Zeitpunkt an dem die Maus über einem Link von Interesse liegt, Mausklicks, die verbrachte Zeit in Bereichen von Interesse und die Dauer in der die Maus über diesem Bereich „schwebt“. Darüber hinaus bieten einige Tracking-Anwendungen höherwertige Analysen, wie Heat-Maps und Play-backs, welche die „Flugbahn“ der Maus zurückverfolgen kann (vgl. [ATTE06]).

```
141.84.8.77 2005-10-25,11:5:57 http://www.kiko.com/ serverdata 12
141.84.8.77 2005-10-25,11:5:58 http://www.kiko.com/ load width=1280;height=867
141.84.8.77 2005-10-25,11:6:2 http://www.kiko.com/ mousemove x=672;y=7
141.84.8.77 2005-10-25,11:6:2 http://www.kiko.com/ mouseover x=731;y=457 target=link:http://www.kiko.com/contact.htm+linktext:Contact
141.84.8.77 2005-10-25,11:6:6 http://www.kiko.com/ click x=815;y=231 target=id:SPAN16
141.84.8.77 2005-10-25,11:6:37 http://www.kiko.com/app.htm?use auth=678397351 mousemove x=849;y=352
141.84.8.77 2005-10-25,11:6:37 http://www.kiko.com/app.htm?use auth=678397351 mouseover x=472;y=296 target=id:DIV144
141.84.8.77 2005-10-25,11:6:37 http://www.kiko.com/app.htm?use auth=678397351 mouseover x=161;y=229 target=id:left bar
141.84.8.77 2005-10-25,11:6:38 http://www.kiko.com/app.htm?use auth=678397351 click x=147;y=183 target=unknown:scrollbar
141.84.8.77 2005-10-25,11:6:40 http://www.kiko.com/app.htm?use auth=678397351 mousemove x=148;y=138
141.84.8.77 2005-10-25,11:6:50 http://www.kiko.com/app.htm?use auth=678397351 click x=26;y=507 target=id:IMG14
141.84.8.77 2005-10-25,11:6:50 http://www.kiko.com/app.htm?use auth=678397351 focus
141.84.8.77 2005-10-25,11:6:56 http://www.kiko.com/app.htm?use auth=678397351 keypress key=T
141.84.8.77 2005-10-25,11:6:56 http://www.kiko.com/app.htm?use auth=678397351 keypress key=e
141.84.8.77 2005-10-25,11:6:56 http://www.kiko.com/app.htm?use auth=678397351 keypress key
```

Abbildung 4: Beispiel eines Ausgabeprotokolls (vgl. [ATTE06])

2.3 Datenschutz

Die Frage nach den rechtlichen Handlungsspielräumen in Bezug auf personenbezogene Daten, solche die in Zusammenhang mit der Nutzung oder Offenlegung von Identitäten oder Handlungen einer Person erfolgen, stellt sich aus datenschutzrechtlicher Sicht immer bei der automatisierten Verarbeitung dieser Daten.

Unter personenbezogenen Daten versteht man nach Definition des Bundesdatenschutzgesetztes (BDSG) Informationen bzw. einzelne Angaben über persönliche oder sachliche Verhältnisse einer bestimmten Person (§ 3 Abs. 1 BDSG). Hierzu zählen unter anderem Angaben wie der Name, das Alter, das Geburtsdatum, Telefonnummern, sowie persönliche E-Mail-Adressen. Des Weiteren werden die „besonderen Arten“ personenbezogener Daten im Sinne des §3 Abs. 9 BDSG noch weiter unterklassifiziert. Zu diesen herausgehobenen, schützenswerten Angaben zählen zum Beispiel die ethnische Herkunft, Angaben zu Gesundheit und Sexualität, oder auch die politische Meinung.

In Deutschland regelt das Telemediengesetz (TMG) die rechtlichen Rahmenbedingungen für sogenannte Telemedien und es ist eine der zentralen Vorschriften des Internetrechts. Hier lassen sich zudem besondere Regeln zum Umgang mit personenbezogenen Daten im Online-Bereich finden. Eine weltweit fast einzigartige Vorschrift betrifft die Verarbeitung der digitalen Nutzungsdaten, welche zum Zwecke der Werbung oder Marktforschung einwilligungslos in Nutzungsprofilen erhoben werden. Diese werden unter Verwendung von Pseudonymen erstellt und verarbeitet (§ 15 Abs.3 TMG).

Mittels Cookies können sehr unterschiedliche Informationen über einen bestimmten Nutzungszeitraum hinweg gesammelt und gespeichert werden. In den Fällen, bei denen Nutzungsdaten mit personenbezogenen Informationen anfallen, gelten zur Verarbeitung die Vorgaben des deutschen Datenschutzrechts. Eine Regelung im TMG, die sich ausdrücklich auf Cookies bezieht gibt es nicht. Allerdings besteht eine gewisse Informationspflicht, die auf den Webseiten-Betreiber zukommt, wenn die eingesetzten Verfahren seinerseits personenbezogene Daten erheben und verarbeiten.

„Der Dienstanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) 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 oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein."

Abbildung 5: § 13 Abs. 1 TMG

Auf Ersuchen des Europäischen Parlaments, sollen die neuen Bestimmungen der sogenannten „Cookie-Richtlinie" mehr Transparenz und Sicherheit für die Verbraucher schaffen. Die neuen Maßnahmen sollten dabei kein eigenes, neues Regelwerk bilden, sondern sahen Änderungen und Anpassungen der Verordnung (EG) Nr. 200/2004 sowie zweier, bereits bestehender Richtlinien, den Richtlinien 2002/22/EG (Universaldienstrichtlinie) und 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) vor. Von besonderem Interesse für die digitale Wirtschaft sind dabei die letztgenannte Richtlinie (sog. genannte E-Privacy-Richtlinie) und deren vorgesehenen Änderungen. Konkret geht es um die neu eingefügten Datenschutz-Vorgaben hinsichtlich der Voraussetzungen für die Einsatzbedingungen von auf dem Endgerät eines Nutzers gespeicherten Informationen. Im Verlauf der Änderungen wurde insbesondere Art. 5 Abs. 3 der E-Privacy-Richtlinie neu verfasst:

"(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."

Abbildung 6: Art. 5 Abs. 3 E-Privacy-Richtlinie

Die Informationen, die in diesem Abschnitt der E-Privacy-Richtlinie der EU bezeichnet werden, können auf verschiedene Weise gespeichert und ausgelesen werden. Cookies sind hier nur eine, aber wohl die bekannteste Art der Verbreitungsmöglichkeiten. Aus diesem Grunde hat sich schnell der Begriff „Cookie-Richtlinie“ durchgesetzt.

Die Richtlinie verlangt strikte Zustimmung des Nutzers zu den bezeichneten Aktivitäten - beispielsweise für das Setzen und Auslesen von Cookies auf dem Computer des Benutzers. Vor der Einwilligung soll der Nutzer umfassend informiert werden. Ihm sollen einfach verständliche Informationen zu Tätigkeiten, die eine Speicherung oder einem Zugriff bedürfen, bereitgestellt werden. Die Benutzerfreundlichkeit soll hier an erster Stelle stehen, damit auch der Materie-ferne Nutzer optimal informiert werden kann.

Die Artikel-29-Datenschutzgruppe, welche sich aus Vertretern der nationalen Datenschutzbehörden, der europäischen Datenschutzbeauftragten (EDSB) und der Europäischen Kommission zusammensetzt, hat darauf hingewiesen, dass die von der Richtlinie geforderte Einwilligung immer einer aktiven Handlung bedarf, um wirksam zu sein (vgl. [ARTI11]). Ein nachträgliches Einverständnis sei dafür nicht

ausreichend. Folgende Möglichkeiten kämen nach Ansicht der Arbeitsgruppe dafür in Frage:

- Der Nutzer kann nach eingespielter Aufklärung über die verwendeten Cookies auf einer vorgeschalteten Webseite („splash screen“) seine Zustimmung erteilen
- Die Zustimmungs-Option auf einem Banner („static information banner“) am oberen Rand der Webseite, wobei jenes auf die jeweilige Datenschutzrichtlinie verweist
- Als Standard vor der Aktivierung der Tracking-Funktion sind Social Plug-Ins vorerst deaktiviert.

Dies bedeutet nicht, dass die Zustimmung des Nutzers nicht auch anders als durch Klicken einer geeigneten Option (Opt-In) erklärt werden kann. Ist der Browser so eingestellt, dass Cookies automatisch zugelassen werden, dann soll dies einer wirksamen Handlung für die Zustimmung der Informationserhebung entsprechen.

Hieraus erschließt sich, dass nach der E-Privacy-Richtlinie der Nutzer über den Einsatz und Nutzen von Cookies informiert sein und er seine Einwilligung geben muss. Die Einwilligung muss bewusst erteilt und protokolliert werden. Außerdem muss der Inhalt der Einwilligung jederzeit für den Nutzer abrufbar und revidiert werden können. Während der Nutzer informiert wird, muss zusätzlich auf das Widerrufsrecht hingewiesen werden (vgl. § 13 Abs. 3 TMG), denn Cookies werden als automatisches Verfahren im Sinne des § 13 Abs. 1 Satz 2 TMG betrachtet. Allerdings gibt es im deutschen TMG keine ausdrücklichen Passagen die sich auf Cookies als solche beziehen.

Als letzte Ergänzung ist die Erstellung von Nutzerprofilen für Werbezwecke zu betrachten. Nach § 15 Abs. 3 TMG (nachfolgend aufgeführt) dürfen solche Profile unter Verwendung von Pseudonymen über den Benutzer ohne dessen Zustimmung erstellt werden, wenn der Benutzer im Zuge der Widerspruchsrechtsbelehrung keine Einwände erhoben hat.

"Der Dienstanbieter 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 Dienstanbieter 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. "

Abbildung 7: § 15 Abs. 3 TMG

Damit sieht § 15 Abs. 3 TMG als Ausnahme von der allgemeinen Forderung der Einwilligung deutlich ein Opt-Out-Verfahren zur Erstellung von Benutzerprofilen für die Werbung vor. Wenn Cookies also für das Werbetracking eingesetzt werden, wie es gewöhnlich der Fall ist, ist nach den gesetzlichen Bestimmungen das Opt-Out-Verfahren ausreichend. Auffällig ist hier, dass die Cookie-Richtlinie eine Zustimmung fordert, während § 15 Abs. 3 TMG dazu widersprüchlich aufgestellt ist. Anhand eines Beispiels lässt sich jedoch zeigen, dass die Regelung im TMG und der Cookie-Richtlinie sich nicht widersprechen. Der Nutzer kann also durch den Verbleib auf einer Webseite, das Weitersurfen und den nicht getätigten Widerspruch eine Zustimmung erteilen, denn eine solche Einwilligung muss nicht durch das Auswählen einer Checkbox getätigt werden. Die Deutlichkeit und Prägnanz der Information über die Cookies, bzw. der Hinweis spielen also eine sehr große Rolle. Dennoch herrscht in der Praxis nach wie vor Unklarheit über regelkonformen Umgang und Auslegung der Vorschriften des deutschen Telemediengesetztes (vgl. [BAUE15]).

3 Konzept

Das dritte Kapitel befasst sich mit der Erstellung des eigentlichen Konzepts. Zuerst werden die wesentlichen Elemente der Konzepterstellung vorgestellt (3.1). Anschließend werden nach diesem Schema die Grundlagen zu einer Strategie (3.4) aufgearbeitet, welche wiederum als Basis für die Realisierung (3.5) dient. Abschließend werden die Ergebnisse zusammengefasst (3.6).

3.1 Verwendete Methodik

Ein Konzept ist eine weit verbreitete Methode, wenn ein Vorhaben konkretisiert werden soll. Je nach Umfang und Art der Unternehmung sind die verschiedenen Kategorien eines Konzepts mehr oder weniger umfassend auszufüllen. Festzuhalten ist, dass es nicht „das“ Vorgehen für die Erstellung eines Konzepts gibt. Als Grundlage dienen diesem Konzept folgende wesentliche Elemente (vgl. [BOJA15]):

1. Kurze Zusammenfassung des Vorhabens

Die Zusammenfassung wird dazu beitragen, die wesentlichen Teile des Konzepts darzustellen und nicht den Gesamtüberblick zu verlieren.

2. Ausgangslage

Die Ausgangssituation sollte verständlich wiedergespiegelt werden und darlegen warum das Projekt relevant und notwendig ist.

3. Strategie

Zur Strategie zählen Zielsetzung, Wirkung und Zielgruppe des Vorhabens. Eine Definition der Ziele, die in Ober- und konkrete Unterziele aufgespalten werden können. Um die Wirkung zu prognostizieren, sollte die Frage beantwortet werden,

welche Auswirkungen mit der Umsetzung des Vorhabens zu erwarten sind. Außerdem ist eine klare Definition der Zielgruppe in Bezug auf die Quantifizierbarkeit des Vorhabens wichtig.

4. Realisierung

Dieser Abschnitt beschreibt, wie das Projekt umgesetzt werden kann und welche spezifischen Aktivitäten geplant sind.

3.2 Kurzfassung

Dieses Konzept befasst sich mit der Entwicklung einer Grundlage für eine Monitoring-Anwendung für Cookies und andere Tracker auf Webseiten. Mit Hilfe eines Überblicks über die aktuelle Marktlage, wird eine Strategie erarbeitet, welche wiederum förderlich für die Realisierung ist.

3.3 Ausgangslage

Mit der jüngsten europäischen Datenschutzrichtlinie für Cookies wurde es wichtig, zu verstehen, welche Cookies eine Webseite erstellt und wann. Es kam zu der Idee ein Tracker-Audit (allgemein ein Untersuchungsverfahren) für Betreiber von Webseiten anzubieten, sowie mit einer Übersichts-Anwendung den Internet-Nutzern ein besseres Verständnis zu liefern. Es muss also ein sehr agiler Prozess gestaltet werden, welches für die Online-Branche allerdings kein Neuland ist. Zudem existieren auf dem Markt schon Anwendungen, welche die systematische Erfassung, Beobachtung und/ oder Überwachung von Cookies vornehmen. Nachfolgend werden das Cookie-Management von Firebug und die Tracker-Datenbank von Ghostery beschrieben.

Wettbewerbsanalyse

Auf dem Markt für Monitoring-Programme werden hauptsächlich Anwendung in Form von Browser-Plug-Ins/-Erweiterungen angeboten. Ein weitverbreitetes Programm, mit aktuell über 2,7 Million Nutzer weltweit (vgl. [MOZI15b]), ist dabei der Firebug, eine Ergänzung für den Webbrowser Mozilla Firefox. Das Programm ermöglicht das Aufrufen einer Fülle von Web-Entwicklungs-Anwendungen während der Benutzer im Internet surft. Seiten und Skripte können bearbeitet, debuggt und das Überwachen von CSS-, HTML- und JavaScript-Inhalten kann vorgenommen werden (vgl. [MOZI15]).
Mit dem Cookie-Management von Firebug können Cookies im Browser anzeigt und verwaltet werden. Eine Detailansicht der Werte und eine Suchfunktion innerhalb der Anwendung ermöglichen dem Nutzer eine erleichterte Anzeige der Cookies. Zudem kann der Zugriff auf Cookies für bestimmte Webseiten verweigert werden. Die Cookies können gefiltert, neu und eigenhändig erstellt werden und vorhandene Cookies können gelöscht werden. Mit der Monitoring-Funktion des Cookie-Managements kann der Benutzer sich seine Cookies nach Werten spaltenweise sortiert anzeigen lassen und anschließend als Text-Datei (.txt) exportieren. Zusätzlich steht ein Feld für die Überwachung des HTTP-Datenverkehrs über Request-/ Response-Round-Trip-Time zur Verfügung. Werden die Werte eines Cookies in JSON- (JavaScript Object Notation, ein kompaktes Datenformat in einer einfach lesbaren Textform zum Zweck des Datenaustauschs zwischen Anwendungen) formatiert, so werden sie anschließend in einer Baumstruktur angezeigt. Außerdem werden Werte von Cookies im XML-Format farblich aufbereitet dargestellt. Ergänzend ist der Einsatz eines Debuggers möglich. Wenn bestimmte Cookies ihre Werte ändern, wird mit Hilfe eines Breakpoints die Zeile des Skripts angezeigt, welche die Änderung verursacht hat. Um feststellen zu können welcher Cookie modifiziert wurde, sowie zum Diagnostizieren und Auffinden von Fehlern ist der Debugger eine hilfreiche Funktion des Programms (vgl. [MOZI15a]).

Neben Firebug gibt es noch einen zweiten, großen und für diese Arbeit interessanten Wettbewerber, mit aktuell 2,2 Millionen Nutzern im Google Chrome Browser (vgl. [GOOG15]), am Markt: Ghostery.

Ghostery ist ebenfalls eine Browser-Erweiterung, also eine App für Browser, Handy oder Tablet. Es zeigt dem Benutzer alle Unternehmen an, die ihm folgen, wenn dieser eine Webseite besucht. Mit Ghostery kann mehr über diese Unternehmen in Erfahrung gebracht werden, zum Beispiel welche Art von Daten sie über den Nutzer erfassen. Außerdem kann das Sammeln der Daten blockiert werden.

Ghostery besitzt eine eigene Tracker-Datenbank und gleicht diese mit Hilfe von Datenerfassungsprogrammen mit all den verschiedenen Web-Servern ab, die von einer bestimmten Webseite aus abgerufen werden. Wenn es zu einer Übereinstimmung gekommen ist, wird das Unternehmen zu einer speziellen Liste hinzugefügt. Falls Ghostery so konfiguriert wurde, dass die Kommunikation mit einem oder mehreren dieser Unternehmen blockiert werden soll, wird diese Abfrage des Browsers unterbrochen. Der Nutzer kann selbst entscheiden, ob er einzelne Tracker, die Tracker einzelner Webseiten oder eine Mischung aus beidem blockieren möchte. Eine Blockierung kann jederzeit wieder aufgehoben werden. Durch das Anlegen von detaillierten Tracker-Profilen kann der Nutzer sehen, was er blockiert hat und sich anhand der von Ghostery erstellten Tracker-Profile über die jeweiligen Unternehmen, die sein Surfverhalten verfolgen, informieren. Neben der Standardausstattung bietet Ghostery die Erweiterung durch Ghostrank. Wenn ein Nutzer Ghostrank aktiviert, werden folgende Informationen erfasst (vgl. [GHOS15]):

- die Tracker, die durch Ghostery identifiziert wurden
- die Seite, auf der diese Tracker gefunden wurden
- das Protokoll der Seite, in dem Tracker gefunden wurden
- der Blockierungsstatus des Trackers
- die erkannten Domänen, die Tracker setzen
- die Ladezeit für Seite und Tracker
- Die Trackerposition auf der Seite
- der Browser, in dem Ghostery installiert wurde
- Information über die Ghostery-Version
- Standard-Serverlog Informationen, wie IP-Adresse und HTTP-Kopfzeilen

Neben den hier vorgestellten Monitoring-Anwendungen Firebug und Ghostery gibt es noch weitere Programme, wie die DebugBar für den Internet Explorer (vgl.

[RABA15]) oder die Opera Dragonfly (vgl. [OPER15]). Diese Webanwendungen unterscheiden sich in Funktionen und Arbeitsweisen nicht weit von den oben genannten Anwendungen und werden daher nicht weiter ausgeführt.

3.4 Strategie

Die EU-Datenschutzrichtlinie hat zunächst eingeführt, dass eine Zustimmung als Voraussetzung für die Speicherung von Informationen auf dem Gerät eines Benutzers vorliegen muss (vgl. Kapitel 2.3). Die vorherrschende Technologie, um solche Informationen zu speichern und anschließend darauf zugreifen zu können sind bis dato die Cookies. Allerdings muss ebenfalls in Betracht gezogen werden, dass Cookies allein nicht mehr ausreichen, auf andere Tracking-Möglichkeiten ausgewichen und um diese ergänzt werden muss. Da die Richtlinie Ausnahmen bezüglich des Zustimmungserfordernisses enthält, ist eine Klassifizierung und Einigung über Cookies und andere Tracker von entscheidender Bedeutung in der Praxis. Für die Erstellung des Konzepts ist im Vorwege eine Klassifizierung zu erstellen. Einige vorgeschlagene Klassifizierungen sind zu streng und reagieren mehr auf eine legalistische Anwendung, anstatt auf die Erwartungen der Verbraucher oder einen pragmatischen Ansatz. Einzelne Organisationen haben auf diese Herausforderung mit der Schaffung von Cookie-Gruppen geantwortet. Während die verschiedenen Kategorisierungen einige Ähnlichkeiten aufzeigen, gibt es Unterschiede bezüglich der Inhalte in den Bereichen. Die Klassifizierung, die sich vorherrschend finden lässt, kategorisiert Cookies in vier bis fünf Gruppen:

- Streng-notwendige Cookies
- Funktionale Cookies
- Performance/ Targeting/ Analytics Cookies
- Tracker/ Online Behavioral Advertising (OBA)/ Registration/ Widgets/ Werbung/ Cookies von Drittanbietern

Während in der Theorie eine einfache Klassifizierung entlang des Rechtes (welche Cookies sind befreit, welche Cookies erfordern Zustimmung) dem Gesetz dienen würde, zeigt ein pragmatischer Ansatz die Notwendigkeit zu unterscheiden und die

Transparenz für den Verbraucher zu erhöhen. Eine weitere Schwierigkeit befasst sich mit der Klassifizierung anderer Tracker. Diese kann allerdings anhand der zuvor erstellen Klassifizierung der Cookies erfolgen, sodass die Kategorien übernommen und um andere Tracker erweitert werden. Die Kategorien sollen hinterher sowohl Cookies, als auch Tracker enthalten und zusammenfassen.

Die oben aufgeführte Liste, vor allem in den letzten beiden Punkten, zeigt die großen Unterschiede in der Interpretation. Dies führt nicht nur zu Verwirrung bei den Verbrauchern, sondern auch bei den Klein- und Mittelständischen Unternehmen (KMU). Insbesondere die KMUs verfügen oft nicht über das Wissen, um die gesetzlichen Anforderungen zu verstehen, beziehungsweise umzusetzen und könnten durch einen allgemein anerkannten Industriestandard unterstützt werden. Solch ein breit akzeptierter Standard sollte eine einfach zu verstehende Klassifikation bereitstellen und fünf Kategorien nicht überschreiten. Bei der Gestaltung des Entwurfs sollte eine Reduzierung auf das Wesentlich, hier die fünf Kategorien, vorgenommen werden, damit die Aussagekraft nicht durch Überfrachtung mit nichtssagendem Beiwerk zu unnötiger Komplexität führt. Außerdem sollte der Fokus auf die Schlüsselfrage der Verbraucher gerichtet sein: Ob die gesammelten Informationen (Daten) auch mit anderen Parteien geteilt werden. Für den Verbraucher ist es sinnvoll davon auszugehen, dass Webseiten/ Controller einige Informationen über den Verarbeitungszweck und gemeinsame Nutzung von Informationen erwarten, ohne auf die Besonderheiten der Cookies oder anderer Tracker einzugehen. Bezüglich Tracker und ihrer Einstufung fehlt ein mehr pragmatischer Ansatz, welcher weniger starr an Paragrafen und Vorschriften festhält.

Eine eindeutig festgelegte Klassifizierung von Cookies würde einen differenzierteren Umgang mit Cookies für Verbraucher unterstützen und besser dem Europäischen Recht und den wirtschaftlichen Rahmenbedingungen entsprechen, in denen die Verarbeitung nach Datenschutzbestimmungen relevant ist. Lösungen wie Cookie-Blocker oder sogar Technologien, die alles blockieren könnten, untergraben aber die legitimen Geschäftsmodelle und liefern keine ausreichenden Informationen für den Nutzer.

Das Ziel wäre ein Tracker-Repository, welches für die Öffentlichkeit frei zugänglich und bereit für weitere Verwendung ist. Es sollte auch ein erklärender Teil für die Verbraucher (in fachfremder Sprache) beigefügt sein, welcher die verschiedenen Kategorien, wie die verschiedenen Arten von Trackern erhoben werden und wie die Verwendung der gesammelten Informationen von statten geht, erläutert. Einerseits sollen die Webseitenbetreiber von dem Konzept profitieren. Es kann eine Hilfestellung für die rechtskonforme Einbindung ihrer Inhalte liefern. Andererseits soll es den Nutzern die Möglichkeit bieten bestimmte Gruppen von Trackern zu blockieren, anstatt alle Tracker blockieren zu müssen. Sie könnten selbst entscheiden von welchen Unternehmen sie online verfolgt werden. Webseiten könnten sich bezüglich der Kategorisierung auf einen vereinbarten Standard verlassen und diesen auf ihren Webseiten implementieren. Für KMUs könnten Lösungen zur Verfügung gestellt werden, die sicherstellen würden, dass bestimmte Tracker nicht auf ihren Seiten platziert werden (viele KMUs haben ihre Webseiten nicht vollständig unter Kontrolle und haben nicht die Mittel diese ständig zu überwachen, ob und welche Tracker aktiv sind oder sich letztendlich auf ihren Webseiten befinden). Verbraucher würden Informationen über die unterschiedlichen Arten von Trackern in einer nutzerorientierten Weise auffinden (Verbraucher wollen möglicherweise für Web-Analyse-Zwecke verfolgt werden, wenn es hilft eine Webseite benutzerfreundlicher zu machen, aber entscheiden sich trotzdem dagegen OBA zu akzeptieren).

Mit der Umsetzung der Klassifizierung als Industriestandard, als Bestandteil des Konzepts sind folgende Vorteile als Auswirkung zu erwarten:

- Eine vereinbarte Norm und somit die Begrenzung der Verwirrung der Verbraucher
- Nutzer sind besser informiert und können verstehen wieso Cookies erforderlich sind
- Erhöhung der Transparenz für die Verbraucher, sowie gleichermaßen für KMUs (KMUs könnten sich auf einen Standard verlassen und Lösungen basierend auf ihren Bedürfnissen implementieren)
- Förderung des Marktes für Webseitenlösungen und die daraus resultierende Schaffung neuer Unternehmen

- Unternehmen können zu vergleichbaren Konditionen konkurrieren und so eine Auswahl an Lösungen für die Nutzer bieten und diese nicht mit unterschiedlichen Ansätzen verwirren

- Befähigung eines verbraucherorientierten Regulierungsansatzes für Tracker anstatt eines legalistischen Ansatzes, der nicht auf Verbraucher ausgerichtet ist

Zunächst stellt sich allerdings die Frage, wie man eine Kategorisierung schafft, die vom Markt anerkannt wird. Die Analyse der bestehenden Kategorisierungen hat ergeben, dass der entscheidende Punkt vorerst die Zuordnung der verschiedenen Tracking-Möglichkeiten auf die Kategorien ist. Der Vorteil ist mit bestehenden Kategorisierungen (siehe 2.1.3) zu arbeiten, anstatt Neue vorzuschlagen. Der ICC nach sind folgende vier Kategorien zu erstellen:

- K1 – strictly necessary
- K2 – performance
- K3 – functionality
- K4 – targeting or advertising

Da die in 2.2 vorgestellten Tracking-Methoden sich alle auf die Aufzeichnung und Auswertung von Nutzer-Verhalten im Internet beziehen und das daraus gewonnene Wissen für nutzungsbasierte Online-Werbung verwendet wird, lassen sich die Tracker pauschal in der vierten Kategorie unterbringen.

3.5 Realisierung

Die Umsetzung der Strategie erfolgt in Form einer Monitoring-Anwendung. Wie die Wettbewerbsanalyse zeigt, gibt es schon einige Unternehmen am Markt, welche sich mit der Überwachung und Analyse von Cookies und anderen Trackern auf Webseiten beschäftigen. Für die Realisierung sind anfangs elementare Überlegungen wie die einer groben Architektur vorzunehmen. Nachfolgend ein erster Entwurf:

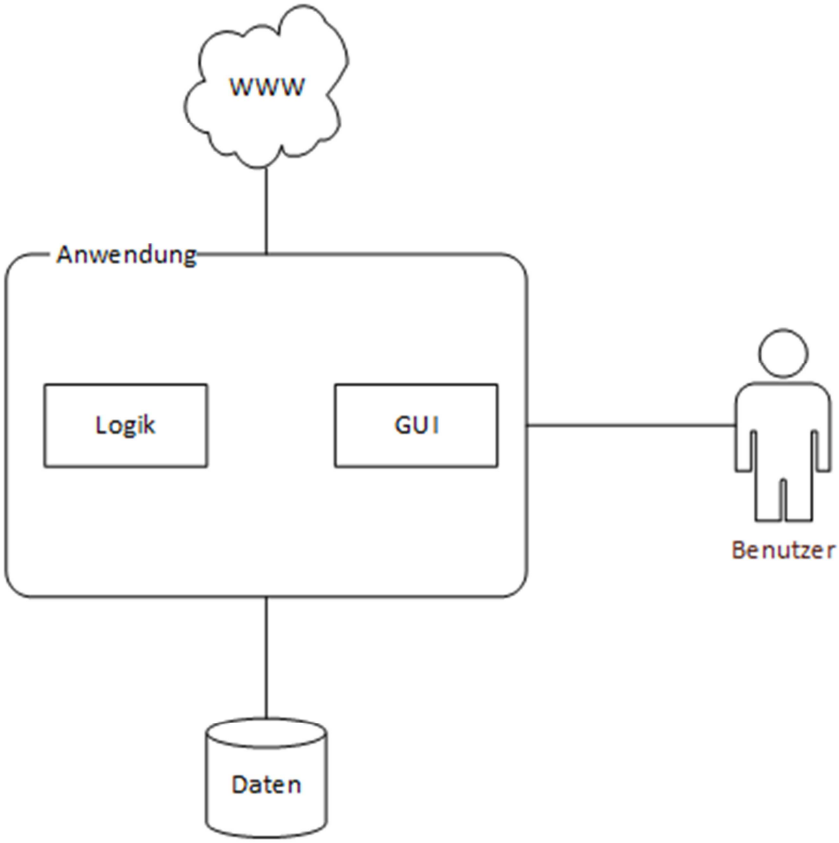

Abbildung 8: Grobe Architektur

Es wird davon ausgegangen, dass die Anwendung sowohl mit dem Internet, als auch mit einer Datenbank und dem Benutzer kommuniziert. Die Anwendung kann auch als eine Webanwendung umgesetzt werden, wobei die Daten in der Cloud

verarbeitet und analysiert werden. Innerhalb der Anwendung verbirgt sich die Logik, welche den Quellcode der Webseite auf die unterschiedlichen Formen von Trackern und Cookies analysiert. Für die Visualisierung der Daten wird die Logik durch eine GUI (vom englischen „graphical user interface“, was übersetzt „grafische Benutzeroberfläche“ bedeutet) ergänzt.

Nun stellt sich die Frage, wie die Cookies und Tracker (nachfolgend zusammengefasst als Tracker) auf den Webseiten überhaupt erkannt werden. Angenommen wird, dass die Anwendung die Tracker anhand ihrer Signaturen und Datenstrukturen im Quellcode erkennen kann. Nach Erkennung eines Trackers müssen diese mit Hilfe der Klassifizierungs-Regeln den verschiedenen Kategorien zugeordnet werden. Ein effektiver Ansatz für die Erstellung der unterschiedlichen und im Laufe der Nutzung anwachsenden Regeln wäre hierbei die Nutzung eines Entscheidungsbaumes. Vergleichbar ist dieses Vorgehen mit dem von Anti-Viren-Programmen. In die Entscheidung der Einordnung können natürlich auch technische Aspekte der Tracker einfließen.

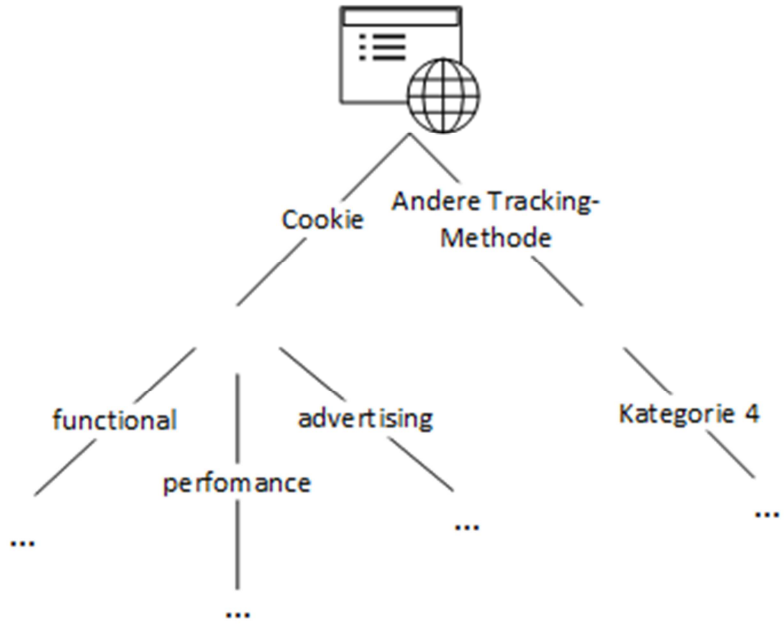

Abbildung 9: Entscheidungsbaum

Ist eine Klassifizierungs-Regel erstellt worden, wird diese in der Datenbank abgelegt und gespeichert. Die Regel kann so auf nachfolgende Tracker angewendet werden, welche die gleichen Kriterien in ihren Signaturen aufweisen. Neben den Klassifizierungsregeln, kann der User eigene benutzerspezifische Regeln erstellen, welche lokal gespeichert werden. Wichtig ist, sich die unterschiedlichen Regeln zu merken. Ist der Benutzer zum Beispiel gerade auf www.amazon.de, möchte aber ein neues Browserfenster mit einer anderen Webseite öffnen, soll diese ebenfalls von der Monitoring-Anwendung analysiert werden, ohne das der zuvor angelegte Warenkorb auf amazon.de vergessen wird. Auf die neue Webseite werden alle Regeln angewendet, ohne das schon bestehende zur Blockierung außer Kraft gesetzt werden. Die Liste mit den Regeln sollte ständig aktualisiert werden, um immer auf dem neusten Stand zu sein. Anschließend wird sie mit dem Browser abgeglichen. Wie der Browser letztlich die detaillierte technische Funktionsweise der Abarbeitung der Trackern vornimmt, beziehungsweise sie daran hindert ihrer Funktion nachzugehen, wird hier nicht weiter behandelt.
Ein tieferer Einblick in die Monitoring-Anwendung zeigt, wie unter Benutzung der Analyse die Webseiten aufgebaut werden können.

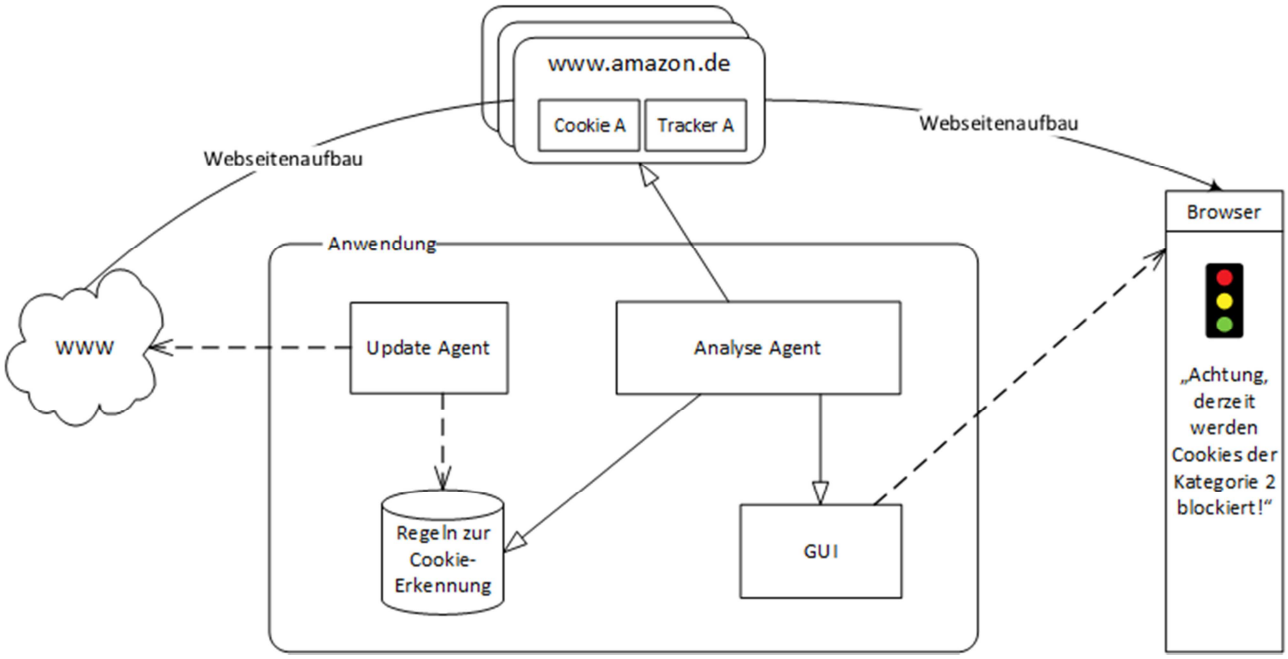

Abbildung 10: Einblick Monitoring-Anwendung

Damit der Vorgang performant und für den Nutzer transparent bleibt, bis sich eine Webseite öffnet, wird die aufzubauende Seite durch den Analyse-Agent überprüft. Dieser Prozess soll durch ein Banner, welches an der Kopfseite des Browsers erscheint, visualisiert werden und den aktuellen Status „Working“ anzeigen. Während der Working-Phase sollen bereits gefundene Ergebnisse angezeigt, beziehungsweise aktualisiert werden. Nachdem die Webseite aufgebaut ist, zeigt die Leiste eine Auskunft über die blockierten Tracker, ihre Einstufung und Information über Tracker dieser Klasse an. Für den Autonormalverbraucher wird die Anzeige durch ein Ampelsystem unterstützt. Der Nutzer kann außerdem selbst entscheiden, wie mit den gefundenen Trackern umgegangen werden soll, beziehungsweise welche er blockiert haben möchte.
Die Monitoring-Anwendung sollte verbreitete Qualitäten der Softwareentwicklung wie Zuverlässigkeit, Effizienz, Wartbarkeit und Änderbarkeit aufweisen. Des Weiteren ist eine hohe Nutzerfreundlichkeit von großer Bedeutung. Diese kann in Form von Usability-Tests sichergestellt werden. Um die Effizienz der Anwendung zu gewährleisten könnten die Regeln und andere Datenbankeinträge über Hashfunktionen rausgesucht werden. Dabei wird ein Hashwert für jedes Objekt der Datenbank berechnet. Diese Hashwerte werden dann in einer kompakten Hashtabelle gespeichert. Bei der Suche braucht jetzt nur der aus der Suchanfrage berechnete Hashwert mit den Einträgen aus der Hashtabelle verglichen werden. Die Datenbanksuche wird durch die Reduzierung des Suchraums über Hashtabellen deutlich beschleunigt (vgl. [SPIT11]). Ein fiktiver Datenbankeintrag könnte wie folgt aussehen:

	Name	Wert	Domain	Gescannter Host	Funddatum	Gültigkeit
1	_kuid_	Iv7KxfnR	.krxd.net	www.bild.de	07.11.2015	179 Tagen
2	POPUPCHECK	1384863955676	www.bild.de	www.bild.de	08.11.2015	22 Stunden

Tabelle 2: Fiktiver Datenbankeintrag der Monitoring-Anwendung

Aus der Tabelle ist zu entnehmen, dass das erste gefundene Cookie ein Third-Party-Cookie ist, da die Domain nicht mit dem gescannten Host übereinstimmt. Außerdem ist es ein Persistent-Cookie. Dieses Cookie würde nach der aufgestellten Klassifizierung also in der vierte Kategorie „Targeting or Advertising“ fallen. Bei dem

zweiten aufgeführten Eintrag handelt es sich um ein First-Party-Cookie. Dieses Cookie fällt voraussichtlich in eine der ersten drei Kategorien. Anhand der hier abgebildeten Daten ist allerdings nicht klar zu erkennen, ob das Cookie notwendig ist, damit der User sich auf der angebotenen Webseite bewegen kann oder es der Funktionalität der Webseite dient.
Eine Regel, die sich aus diesem Fund ergeben könnte, wäre eine First-Party-Regel, welche überprüft, ob die Domain und die überprüfte Domain (eingetragen als gescannter Host) identisch sind.
Abschließend stellt die Frage was mit den Trackern passiert, die nicht eingeordnet werden konnten. Diese sollen über ihre Domain einem Unternehmen zugeordnet werden, welches dann auf seine Aufgaben überprüft wird und anhand derer die Tracker in eine Kategorie eingeordnet werden können.
Eine weitere Überlegung befasst sich mit der Kontrolle durch eine höhere Instanz. Findet die Monitoring-Anwendung einen Tracker, der eindeutig gegen das geltende Recht verstößt, wird dieses Ereignis an eine höhere Instanz, wie zum Beispiel eine Verbraucherschutzorganisation, gesendet.

Zusätzlich ist zu beobachten, was andere Unternehmen bereits auf dem Markt anbieten (siehe 3.3.1). Für den Nutzer sollten eine Detailansicht der identifizierten Tracker, sowie eine Suchfunktion angeboten werden. Außerdem sollte die Monitoring-Anwendung ein einfaches Klicksystem für das Blockieren der Tracker aufweisen. Grundlegend sollte die Anwendung die gleichen Möglichkeiten bieten, sich aber durch Funktionalität und Effektivität einen Wettbewerbsvorteil schaffen. Hier sollte die Anwendung über ein größeres Wissen über die Tracker verfügen, beziehungsweise mehr Tracker kennen als die Konkurrenz. Zunächst kann sich auf die meist genutzten Webseiten, wie Facebook, Amazon und Co., bezogen werden. Wenn die Anwendung zuverlässig auf den ausgewählten Webseiten läuft, sollte eine Testphase unter Einbezug der Nutzer folgen.

4 Schluss

Dieses Kapitel bildet den Abschluss der Bachelorarbeit und fasst die Arbeit und die gewonnenen Erkenntnisse zusammen. Zunächst wird ein Resümee des dritten Kapitels erfolgen. Abschließend bietet das Kapitel einen Ausblick (4.2) auf aktuelle Technologien, welche auf diesem Gebiet von Interesse sein können.

4.1 Zusammenfassung

Das Ziel dieser Bachelorarbeit, ein Konzept zur Überwachung von Cookies und anderen ausgewählten Trackern auf Webseiten auszuarbeiten, sowie erste Grundlagen für eine zu erstellende Anwendung anzufertigen, wurde erreicht. Die Entwicklung des Themas war zu Beginn eine Analyse der Grundlagen, welche im dritten Kapitel in die Ausarbeitung des Konzepts mit eingeflossen sind. Als kurze Zusammenfassung der Ergebnisse muss aufgeführt werden, dass die Erarbeitung der Strategie von besonderer Bedeutung war. Mit der Erstellung einer Klassifizierung für Cookies und andere Tracker kann der nächste, schwierigere Schritt der Durchsetzung als Industriestandard folgen. Ohne eine einheitliche, von der Wirtschaft anerkannte Klassifizierung setzt sich eine Monitoring-Anwendung nicht genügend ab und würde sich in der Fülle der Lösungen von Konkurrenten nicht sichtbar am Markt etablieren.
Der Erfolg dieses Konzepts hängt vor allem davon ab, ob es mit seiner Umsetzung die Kundenbedürfnisse erfüllt, welches wiederum zu einer langfristigen Kundenbindungen führt. Um diese Bindung mit Unternehmen, sowie dem Endverbraucher herzustellen, benötigt die Anwendung eine ständige Aktualisierung der Regeln und Filter, sowie eine später mögliche Erweiterung um speicherbare Reports. Außerdem scheint nicht die Zunahme an neuen Methoden oder Trackern, sondern mehr die stetige Zunahme des Einsatzes der bestehenden Technologien

und damit die Vergrößerung der Datenbasis und der Analysemöglichkeiten das Hauptproblem zu sein.
Dabei spielen stetig sinkende Preise für die Möglichkeiten der Datenspeicherung und die immer schneller werdende Analyse der Daten, durch schnellere Prozessoren, eine Hauptrolle. Ganz im Sinne der Mooreschen Gesetzmäßigkeit wird das Analysieren und Persistieren von großen Datenmengen vergleichsweise immer schneller und kostengünstiger gelöst.
Neben den aufgezeigten Schwachstellen ermöglicht das Konzept Rückschlüsse auf eine optimale Gestaltung und bietet das Potenzial einer Weiterbearbeitung des Geschäftskonzepts. Deutlich ist, dass es durch einen detaillierten Businessplan ergänzt werden muss, welcher die Kosten für die Durchführung des Projekts abschätzen kann. Die Umsetzung dieser Verfahren kann einige Zeit dauern, Zeit die man in der sich ständig ändernden und weiterentwickelnden Online-Branche nicht immer haben könnte.

4.2 Ausblick

Neben dem Setzen von Cookies und anderen Trackern auf Webseiten, sowie mobilen Webseiten ist mit der fortschreitenden Technologie auch das Setzten von Cookies innerhalb von Apps zu betrachten. Dies ist mittels HTML-View schon möglich. Dabei werden Webseiten im Layout einer Applikation angezeigt. Für die Nutzung des Trackings sind aber einige Einschränkungen hinderlich. Die so gesetzten Cookies können nur innerhalb der App ausgelesen werden und dementsprechend gewonnene Informationen sind für andere Apps nicht von Nutzen. Das gezielte Ausspielen von Werbung ist hier gestört. Eine Alternative für das Tracking innerhalb von Apps ist die sogenannte Advertising-ID. Sowohl Android-basierte, als auch iOS-basierte Geräte bedienen sich einer solchen ID. App-Entwickler verwenden den Advertising-Identifier, um das Gerät des Nutzers unter verschiedenen Geräten zu erkennen und dann großzügig zielgerichtete Anzeigen auszuspielen. Basierend auf der Advertising-ID können Entwickler anonyme Benutzerprofile, die Informationen für gezielte Werbung sammeln, erstellen. Die Advertising-ID kann vom Benutzer manuell zurückgesetzt werden. Wird diese Option aktiviert, dürfen Apps die ID nicht mehr benutzen, um personalisierte

Werbung auszuliefern. Da die ID das Gerät identifiziert, können gesammelte Informationen über mehrere Apps hinweg verwendet werden.
Das Apple iOS hat vor Einführung der „ID for Advertisers“ (IDFA) den so genannten Unique Device Identifier (UDID) verwendet. Durch die eindeutige und ewige Gültigkeit brachte der Tracker aber große Datenschutzprobleme mit sich und wurde für das Tracking untersagt. Bei Googles Android war die Situation ähnlich. Anfangs stand zur Identifikation eines Geräts nur die Android-ID zur Verfügung, die analog zur UDID permanent und vom Nutzer nicht zu kontrollieren war. Mit Einführung der Google-Advertising-ID ist aber auch diese für weitere Targeting-Nutzung verboten worden. Die Google-Advertising-ID kann von jeder App verwendet werden, indem von Google-Play-Services bereitgestellte Funktionen eingebaut werden (vgl. [BAUE15]).

Neben den Applikationen auf mobilen Endgeräten findet das Sammeln und Speichern von Information heutzutage auch auf internetfähigen SmartTVs statt. Mit dem etwas unhandlichen Begriff „HbbTV“, welcher für „Hybrid Broadcast Broadband TV“ steht und ein neben dem TV-Programm ausgestrahltes Online-Angebot ist, werden dem Nutzer zusätzliche Funktionen, wie eine ausführliche Programmvorschau oder eine Mediathek für verpasste Sendungen, angeboten. Dies funktioniert über das Aufrufen einer Online-Startseite beim Wechseln der Kanäle. Hier ist aber zwischen den verschiedenen Anbietern zu unterscheiden. Die HbbTV-Server des ZDF fragen beispielsweise nur einmalig den Gerätetyp ab, wohingegen bei ProSieben und RTL die HbbTV-Startseite im Hintergrund weitere Daten sammelt und diese an die Sender, und sogar an Dritte übermittelt. So hat der Online-Statistikdienst Google-Analytics sogar Zugriff auf die gesammelten Nutzerdaten. Das Einsehen von Daten, wie zum Beispiel der IP-Adresse, einer bei Verbindungsaufbau übertragene Kennung des Gerätetyps, oder des ungefähren Standorts, lassen den Anschlussinhaber identifizierbar werden (vgl. [LEUW15]).

Wie die beiden obigen Beispiele zeigen beschränkt sich das Tracking für Werbezwecke nicht mehr nur auf Personal-Computer. Durch weitere Beschäftigung mit dem Thema und dem Konzept kann und sollte eine Monitoring-Anwendung auch für Tracker auf anderen Geräten mit neuen Technologien eingesetzt werden können.

Literaturverzeichnis

[ARTI11]
Article 29 Data Protection Working Party (2011): Opinion 15/2011 on the definition of consent. Adopted on 13 July 2011. 01197/11/EN. Online verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf, zuletzt geprüft am 05.11.2015.

[ATTE06]
Atterer, Richard; Wnuk, Monika; Schmidt, Albrecht (2006): Knowing the User's Every Move – User Activity Tracking for Website Usability Evaluation and Implicit Interaction. Edinburgh, UK. Online verfügbar unter http://fnuked.de/usaproxy/www2006-knowing-the-users-every-move--user-activity-tracking-for-website-usability-evaluation-and-implicit-interaction.pdf, zuletzt geprüft am 17.08.2015.

[BAUE15]
Bauer, Christoph; Breuer, Markus; Diebold, Daniel; uvm. (2015): Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte. Hg. v. Bundesverband Digitale Wirtschaft (BVDW) e.V. Online verfügbar unter http://www.bvdw.org/medien/browsercookies-und-alternative-tracking-technologien-technische-und-datenschutzrechtliche-aspekte?media=7007, zuletzt geprüft am 18.09.2015.

[BEWE14]
Bewersdorff, Jörg (2014): Objektorientierte Programmierung mit JavaScript. Direktstart für Einsteiger. Wiesbaden: Springer Vieweg (SpringerLink : Bücher). Online verfügbar unter http://link.springer.com/book/10.1007/978-3-658-05444-1.

[BOJA15]
bOJA – Bundesweites Netzwerk Offene Jugendarbeit (Hg.): Konzepte schreiben - leicht gemacht! Online verfügbar unter http://www.boja.at/fileadmin/_migrated/content_uploads/konzepte_schreiben_03.pdf, zuletzt geprüft am 02.11.2015.

[BROW15]
BrowserLeaks.com (Hg.) (2015): HTML5 Canvas Fingerprinting. Online verfügbar unter https://www.browserleaks.com/canvas, zuletzt geprüft am 29.07.2015.

[CUTR14]
Cutroni, Justin (2014): Understanding Cross Device Measurement and the User-ID. Online verfügbar unter http://cutroni.com/blog/2014/04/10/understanding-cross-device-measurement-and-the-user-id/, zuletzt aktualisiert am 17.08.2015, zuletzt geprüft am 17.08.2015.

[ECKE10]
Eckersley, Peter (2010): How Unique Is Your Web Browser? In: Mikhail J. Atallah, Nicholas J. Hopper (Hg.): Privacy enhancing technologies. 10th International Symposium, PETS 2010, Berlin, Germany, July 21-23, 2010. Proceedings. Berlin, Heidelberg: Springer-Verlag (LNCS sublibrary. SL 4, Security and cryptology, 6205), S. 1–18. Online verfügbar unter https://panopticlick.eff.org/browser-uniqueness.pdf, zuletzt geprüft am 02.11.2015.

[GHOS15]
Ghostery, Inc. (Hg.): GHOSTERY - Ghostery Browser Extension Privacy Statement. Online verfügbar unter https://www.ghostery.com/about-us/privacy-statements/ghostery-browser-extension/ghostery-browser-extension-privacy-statement/, zuletzt geprüft am 19.10.2015.

[GOOG15]
Google (Hg.): chrome web store. Ghostery. Online verfügbar unter https://chrome.google.com/webstore/detail/ghostery/mlomiejdfkolichcflejclcbmpeaniij/reviews?hl=en, zuletzt geprüft am 30.11.2015.

[GOOG15a]
Google (Hg.) (2015): Benutzerdefinierte Gadgets: Richtlinien für Entwickler - YouTube-Hilfe. Online verfügbar unter https://support.google.com/youtube/answer/1727240?hl=de, zuletzt geprüft am 11.11.2015.

[GOVE14]
Governor Technology Ltd. (Hg.): Types of cookies. Online verfügbar unter http://cookiepedia.co.uk/types-of-cookies, zuletzt geprüft am 16.05.2015.

[HUAN11]
Huang, Jeff; W. White, Ryen; Dumais, Susan (2011): No Clicks, No Problem: Using Cursor Movements to Understand and Improve Search. Online verfügbar unter http://jeffhuang.com/Final_CursorBehavior_CHI11.pdf, zuletzt geprüft am 17.08.2015.

[ICCU12]
International Chamber of Commerce UK (ICC UK) (April 2012): ICC UK Cookie guide. ICC United Kingdom, info@international-chamber.co.uk. Online verfügbar unter http://www.international-chamber.co.uk/components/com_wordpress/wp/wp-content/uploads/2012/04/icc_uk_cookie_guide.pdf.

[KRAS10]
Kraska, Sebastian (2010): FLASH-COOKIES: ZOMBIES IM DATENSCHUTZRECHT? Hg. v. Sebastian Kraska. Online verfügbar unter http://www.datenschutzbeauftragter-online.de/datenschutz-flash-cookies-zombies-datenschutzrecht/, zuletzt geprüft am 26.06.2015.

[KRUE07]
Krüger, Jan Fabian (2007): Flash-Cookies: Datensammler der nächsten Generation. Hg. v. PCFreunde.de. Corvios GmbH. Online verfügbar unter http://www.pcfreunde.de/artikel/a61/flash-cookies-datensammler-der-naechsten-generation/, zuletzt geprüft am 26.06.2015.

[LEUW15]
Leuw, Christoph de; Plöger, Steven (2015): Datenkrake Smart TV: Klage gegen Samsung. Datenkrake im Wohnzimmer? Hg. v. COMPUTER BILD. Online verfügbar unter http://www.computerbild.de/artikel/cb-News-Smart-TVs-Samsung-Klage-Daten-9216909.html, zuletzt geprüft am 13.11.2015.

[MAND11]
Mandalka, Markus (o.J. [2011]): Tracking verhindern: Schutz vor Ausforschung Ihrer Internetaktivitäten. Online verfügbar unter http://www.selbstdatenschutz.info/tracking_verhindern/, zuletzt geprüft am 06.05.2015.

[MITT10]
Mittal, Sonal (2010): User Privacy and the Evolution of Third-Party Tracking Mechanisms on the World Wide Web. In: SSRN Journal. DOI: 10.2139/ssrn.2005252.

[MOZI15]
Mozilla Corporation (Hg.): What is Firebug? : Firebug. Online verfügbar unter http://getfirebug.com/whatisfirebug, zuletzt geprüft am 02.10.2015.

[MOZI15a]
Mozilla Corporation (Hg.): Cookie Management : Firebug. Online verfügbar unter http://getfirebug.com/cookies, zuletzt geprüft am 02.10.2015.

[MOZI15b]
Mozilla Foundation [US]: ADD-ONS. Erweiterungen. Hg. v. Mozilla Corporation. Online verfügbar unter https://addons.mozilla.org/de/firefox/addon/firebug/, zuletzt geprüft am 30.11.2015.

[NIKI14]
Nikiforakis, Nick; Acar, Günes (2014): Browser Fingerprinting and the Online-Tracking Arms Race. Web advertisers are stealthily monitoring our browsing habits—even when we tell them not to. Hg. v. IEEE Spectrum. Online verfügbar unter http://spectrum.ieee.org/computing/software/browser-fingerprinting-and-the-onlinetracking-arms-race, zuletzt geprüft am 02.11.2015.

[ONPA15]
OnPage.org GmbH (Hg.) (2015): Cross-Device Tracking. Online verfügbar unter https://de.onpage.org/wiki/Cross-Device_Tracking, zuletzt aktualisiert am 14.08.2015, zuletzt geprüft am 17.08.2015.

[ONPA15a]
OnPage.org GmbH (Hg.) (2015): Canvas Fingerprinting. Online verfügbar unter https://de.onpage.org/wiki/Canvas_Fingerprinting, zuletzt aktualisiert am 09.07.2015, zuletzt geprüft am 25.07.2015.

[ONPA15b]
OnPage.org GmbH (Hg.) (2015): Tracking Pixel. Online verfügbar unter https://de.onpage.org/wiki/Tracking_Pixel, zuletzt aktualisiert am 07.08.2015, zuletzt geprüft am 08.08.2015.

[OPER15]
Opera Software (Hg.) (2015): Opera Dragonfly. Fast, lean and powerful. Meet Opera Dragonfly — our fully-featured suite of developer tools, designed to make your job easier. It's just a right-click away. No install required. Online verfügbar unter http://www.opera.com/dragonfly/, zuletzt geprüft am 30.11.2015.

[RABA15]
Rabaute, Jean-Fabrice (2015): DebugBar - IE extension for web developer : DOM inspector, Javascript debugger, HTTP headers viewer, Cookies viewer. Hg. v. Core Services. Online verfügbar unter http://www.debugbar.com/, zuletzt geprüft am 30.11.2015.

[ROET99]
Rötzer, Florian (1999): Nach den Cookies die Web Bugs. Hg. v. Heise Medien. Online verfügbar unter http://www.heise.de/tp/artikel/5/5482/1.html, zuletzt aktualisiert am 08.08.2015, zuletzt geprüft am 10.08.2015.

[SCHN14]
Schneider, Markus; Enzmann, Matthias; Stopczynski, Martin (2014): Web-Tracking-Report 2014. Hg. v. Michael Waidner. Fraunhofer-Institut für Sichere Informationstechnologie SIT, zuletzt geprüft am 28.08.2015.

[SCHO12]
Schönherr, Maximilian; Kloiber, Manfred (2012): Die Cookie-Bäcker. Hg. v. Deutschlandfunk. Deutschlandradio. Online verfügbar unter http://www.deutschlandfunk.de/die-cookie-baecker.684.de.html?dram:article_id=43115, zuletzt geprüft am 26.06.2015.

[SCHU14]
Schukay, Ralf: Universal Analytics – Das neue Google-Analytics mit Cross-Device-Tracking. Hg. v. mediaworx berlin AG. Online verfügbar unter http://chili-conversion.de/universal-analytics-cross-domain-tracking/, zuletzt geprüft am 17.08.2015.

[SPIT11]
Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim (2011): Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen: Vieweg+Teubner Verlag. S. 95-108. Online verfügbar unter https://books.google.de/books?id=psAhBAAAQBAJ, zuletzt geprüft am 02.12.2015.

[STAH12]
Stahl, Ernst (2012): E-Commerce-Leitfaden. Noch erfolgreicher im elektronischen Handel. 3., vollst. überarb. und erw. Aufl. Regensburg: Univ.-Verl. Regensburg (ibi research an der Universität Regensburg). Online verfügbar unter http://www.ecommerce-leitfaden.de/lasst-zahlen-sprechen.html#anchor_3_3, zuletzt geprüft am 17.08.2015.

[WALT08]
Walter, Thomas (2008): Kompendium der Web-Programmierung. Dynamische Web-Sites; mit 22 Tabellen. Berlin: Springer-Verlag Berlin Heidelberg (X.media.press). Online verfügbar unter http://link.springer.com/book/10.1007/978-3-540-33135-3, zuletzt geprüft am 16.05.2015.

[WORL15]
World Wide Web Consortium (W3C) (Hg.) (2015): Web Storage (Second Edition). W3C Proposed Recommendation 26 November 2015. Online verfügbar unter http://www.w3.org/TR/webstorage/, zuletzt aktualisiert am 25.11.2015, zuletzt geprüft am 27.11.2015.

Versicherung über Selbstständigkeit

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, den _____ _____