Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Seminararbeit

Kathrin Baitinger

Cookie basierte Tracking-Techniken

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Kathrin Baitinger

Cookie basierte Tracking-Techniken

Seminararbeit zum Thema: „Cookie basierte Tracking-Techniken“
im Studiengang „Next Media“
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg
Matrikel-Nr. 2252474

Betreuender Prüfer : Prof. Dr. Kai von Luck

Eingereicht am 29.02.2016

Kathrin Baitinger

Thema der Ausarbeitung zur Ringvorlesung

Cookie basierte Tracking-Techniken

Stichworte

Datenquellen, HTTP Cookie, Tracking, Evercookie, Canvas Fingerprinting, Adserver

Kurzzusammenfassung

„Big Data“ ist ein aktuell vieldiskutiertes Thema. Diese Ausarbeitung beschreibt die Möglichkeiten, eine riesige Menge personenbezogener Daten während der Internetnutzung zu generieren.

Title of the paper

Cookie based tracking – technology

Keywords

Data sources, HTTP Cookie, Tracking, Evercookie, Canvas Fingerprinting, Adserver

Abstract

"Big Data " is one of the key topics. This draft is about opportunities to collect personal data by tracking internet behavioral.

Inhaltsverzeichnis

1 Einleitung

In unserem Alltag geben wir häufig persönliche Informationen im World Wide Web an. Dies geschieht zum einen bewusst, indem wir beispielsweise unsere Nutzerdaten in Profilen von Social Media Plattformen und Online-Shops angeben, oder durch die Teilnahme an Gewinnspielen und Newsletter-Registrierungen. Ein viel größerer Teil der Datenerhebung erfolgt allerdings intransparent, und für eine Mehrheit der Online-User geschieht dies unbemerkt.

In der folgenden Ausarbeitung möchte ich näher auf die Möglichkeiten der Datenerzeugung eingehen. Hierbei handelt es sich um ein sehr komplexes und stetig wachsendes Themengebiet, daher werde ich mich auf die Cookie basierten Tracking Möglichkeiten fokussieren und die auf der klassischen Cookie-Mechanik basierten Evercookies sowie das Fingerprinting näher betrachten.

2 Datenquellen

Durch unzählige Datenquellen können Informationen über Verhalten, Gewohnheiten, Vorlieben, Standorte und noch vielem mehr des individuellen Users erhoben werden.

Eine Quelle sind beispielsweise Logdateien, hinter denen wir als Nutzer unser persönliches Profil finden und durch diese „Wiedererkennung“ eine sehr benutzerfreundliche Interaktion auf den Seiten vorfinden. Betrachten wir Facebook: Durch meine Anmeldung als Nutzer und Profilinhaber habe ich Facebook ganz transparent meine E-Mail-Adresse genannt, in welchem Land mich aufhalte, in den meisten Fällen auch mein Geschlecht sowie mein Alter. Daß Facebook weitere persönliche Informationen von seinen 1,4 Mrd. Nutzer sammelt, die sich beim Hinzurechnen der ebenfalls zum Konzern gehörenden Social Media Plattformen Instagram und WhatsApp auf einen Datenpool von 2,4 Mrd. Accounts[1] ausweitet, sollte ein offenes Geheimnis sein.

[1] **Wolfie, Christl. FAZ.net. Facebooks Datenauswertung - Verstecken kann sich niemand mehr.** [Online] 28. 04 2015. http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/facebooktracktseinenutzeronlineundoffline13562350p2.html

Facebook greift aus unterschiedlichen Quellen auf ein breites Spektrum von Nutzerdaten zu und ergänzt diese Datensammlung über die detaillierte „Tiefen-Analyse“ des Profilinhabers (vgl. Horizontal and Vertical refers).[2]

Eine weitere Datenquelle stellen die mitgeführten, internetfähigen Geräte wie Smartphones, Tablets oder Laptops dar. Über das Tracken von Geo-Daten, Sensoren-Analyse, IP-Adresse oder der Geräte-Identifikationsnummer lassen sich ebenfalls zahlreiche Informationen generieren. So basiert der Funktionsumfang der Google Maps-App u.a. auf dem Zusammenführen von Smartphone-Informationen der Nutzer im relevanten Umkreis, um neben dem Kartendienst auch Stauwarnungen auszugeben und über eine geschätzte Verweildauer im Stau zu informieren.[3]

Apps stellen ebenfalls eine Quelle für Daten-Tracker dar. Mit der Installation bestätigt der User die Nutzungsbedingungen und oft haben damit viele Apps einen "vollständigen Netzwerkzugriff“. Laut einer französischen Untersuchung[4], haben sich 70% der Apps für Android-Mobiles, mit über 40 externen Datensammlern verbunden. Besonders erwähnenswert ist eine Equalizer-App, mit der Musik-Tuning ermöglicht wird; bei der App konnten ca. 1.000 Tracker nachgewiesen werden.

Auch über die Nutzung von öffentlichen W-LAN Zugängen, Bluetooth Schnittstellen oder Near Field Communication werden Nutzer-Informationen ausgetauscht und preisgegeben.

Einen gigantischen Pool an Datenpunkten erstellen wir zudem mit unserem Suchverhalten und den Suchanfragen im Internet, die zum Großteil über die Google-Suchmaschine erfolgen. Diese bewältigt weltweit täglich etwa 3,5 Milliarden Suchaufträge, die pro Sekunde durchschnittlich 40.500 Anfragen entsprechen.[5] Welche Themen für mich abhängig von Region, Uhrzeit und Kontext relevant sind – diese Fragen kann Google problemlos beantworten. Ergänzend stellen der persönliche Browserverlauf und entsprechende Einstellungen eine Datenquelle dar.

---

[2] **Aleyasen, Amirhossein, et al.** On the Privacy Practices of Just Plain Sites. Denver, Colorado, USA : s.n., 2015. ACM 978-1-4503-3820-2/15/10

[3] **Maps, Google.** The official blog for Google Maps. [Online] 20. 05 2015. http://google-latlong.blogspot.de/2015/05/dont-let-traffic-slow-you-down-this.html

[4] **Vigneriy, Luigi , et al.** Taming the Android AppStore: Lightweight. s.l. : EURECOM, Technicolor Research, 2015. Research Report RR-15-305

[5] **live-counter.com.** [Online] [Zitat vom: 17. 02 2016.] http://www.live-counter.com/google-suchen/

3 Cookies als Datenquelle

Durch den Zugriff auf Webseiten von Dienstleistern, Medienhäusern, Social Media Plattformen, E-Mail-Diensten, Shopping-Anbietern, Kommunikationsplattformen und weiteren Angeboten, die im World Wide Web zur Verfügung stehen, besteht eine permanente Verbindung und Austausch zwischen dem genutzten Endgerät und den Servern sowie Ad-Servern der Dienstleister. Bei diesem beständigen Datentransfer werden eine Vielzahl an Informationen über unterschiedliche Wege ausgetauscht. Eine der bekanntesten und verbreitetsten Varianten ist das Cookie-Tracking.

3.1 HTTP Cookie

Um Webseiten aus dem World Wide Web in einem Webbrowser laden zu können, wird das Hypertext Transfer Protocol (kurz: HTTP) benötigt. Dies ist ein zustandsloses Protokoll, welches die einzelnen Seitenaufrufe des Webservers unabhängig voneinander betrachtet. Man kann folglich sagen, dass dem HTTP keine „Erinnerung“ zugrunde liegt. Damit ein User über mehrere Vorgänge hinweg wiedererkannt wird und auch die persönlichen Einstellungen beibehalten werden, kommen Cookies als „Erinnerungs-Maker“ zum Einsatz.
Nach der klassischen Definition ist ein Cookie eine „Textinformation, die die besuchte Website (hier „Server“) über den Browser im Rechner des Betrachters („Client“) platziert. Der Cookie wird entweder vom Webserver an den Browser gesendet oder von einem Skript (etwa JavaScript) in der Website erzeugt. Der Client sendet die Cookie-Information bei späteren, neuen Besuchen dieser Seite mit jeder Anforderung wieder an den Server.“[6]

So ist es möglich, das User auf einer Internet-Seite wiedererkannt werden und spezifische Einstellungen automatisch hergestellt werden. Auch innerhalb einer Online-Sitzung ermöglichen Cookies einen benutzerfreundlichen Umgang. Wenn im Einkaufswagen eines Online-Shops Produkte gesammelt werden, das Angebot des gesamten Shops allerdings noch weiter besucht wird, so ist es möglich, den Warenkorb mit all seinen Produkten beizubehalten um auch im weiteren Sitzungsverlauf darauf zugreifen zu können.

Cookies können mit jedem Dateiformat übertragen werden, auch über Bilddateien kann eine Implementierung stattfinden.

Um eine gewisse Datenhoheit und –Sicherheit zu gewährleisten, kann immer nur der Server den Cookie lesen, der ihn auch versendet hat. Also nur der Absender hat Zugriff auf den gesetzten Cookie.

[6] **Wikipedia.** [Online] 05. 01 2016. https://de.wikipedia.org/wiki/HTTP-Cookie

Cookies werden genutzt, um dem User die Nutzung der Seite bedienerfreundlich zu gestalten; Passwörter werden gemerkt, die letzte Buchung ist noch einsehbar, der Warenkorb bleibt gefüllt. Natürlich nutzen Seitenbetreiber die Cookies auch zur Erstellung eines Benutzerprofils über das Survverhalten auf den Seiten, zur Erstellung persönlicher Empfehlungen oder auch zur Optimierung der Seiten-Struktur. Bei dieser direkten Beziehung zwischen Seiten-Betreiber, als Cookie-Versender, und dem Nutzer, sprechen wir von First-Party-Cookies. Es gibt aber auch andere Konstellationen, die im weiteren Verlauf beschrieben werden.

3.2 Unterschiedliche Absender von Cookies

Zusammengefasst stellen Cookies eine sehr hilfreiche Technologie dar, bei der wir dennoch zwischen erwünschten und unerwünschten Cookies unterscheiden sollten. Wie Ed Felten bereits 2009 sagte: "…they allow a site to tell when it's seeing the same browser (and therefore, probably, the same user) that it saw before…The dark side of cookies involves "hidden" sites that track your activities across the web."[7]

Oft wird bei Seiten-Aufrufen nicht nur auf den Webserver des Anbieters zugegriffen, sondern ergänzende Inhalte, wie Werbemittel, durch weitere Server eingebettet (vgl. Abb. 1). Auf diesem Weg können eine Vielzahl an Cookies von unterschiedlichen Absendern an den Client gesendet werden. Daher gehört es mittlerweile zur Normalität, dass über den Aufruf einer Homepage, mehrere Cookies zu einem User gelangen. Die kommunizieren wiederum mit ihrem jeweiligen Absender und geben Informationen über den Nutzer preis. Wechselt der User dann beispielsweise durch den Klick auf den Werbebanner von der ursprünglichen Domäne zu der verlinkten Website, kann der AdServer exakt verfolgen, woher der User kommt, wer er ist und ob er eventuell schon einmal da war. Tracking-Cookies die durch Dritte gesetzt werden, werden 3rd-Party-Cookies genannt.[8]

[7] **Felten, Ed.** Freedom to Tinker. [Online] 07. 07 2009. [Zitat vom: 12. 01 2016.] https://freedom-to-tinker.com/blog/felten/if-youre-going-track-me-please-use-cookies/

[8] **Englehardt, Steven, et al., et al.** Cookies That Give You Away:. Florence : International World Wide Web Conference Committee, 2015. ACM 978-1-4503-3469-3/15/05

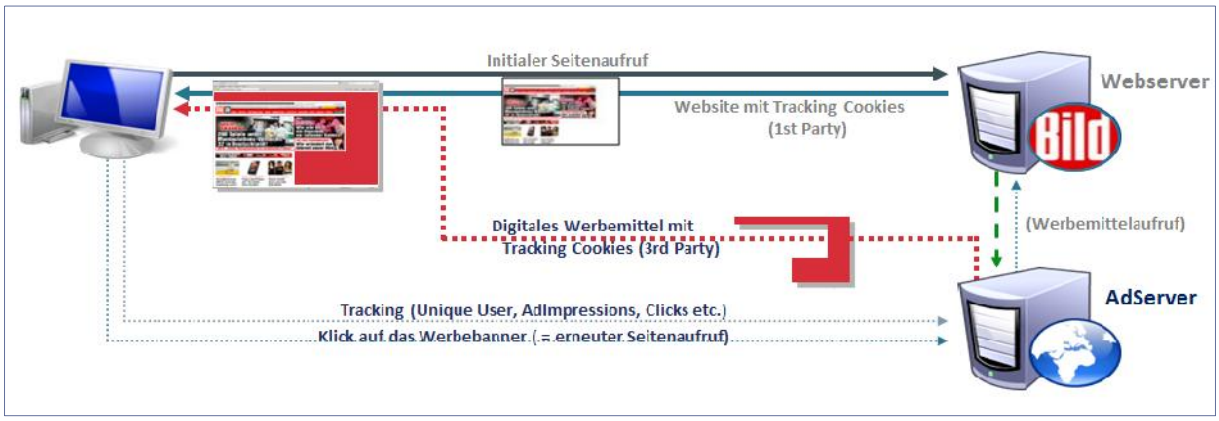

Abb.1: Darstellung der Vernetzungen zwischen Client, Webserver und Adserver

Die Implementierung eines AdServers und dem zusätzlichem Datentracking bietet folgende Vorteile:

- Die Performance von Online-Anbietern in Bezug zu den eingesetzten Werbemitteln kann analysiert werden.
- Die implementierten Werbemittel können mit dem Besucher der Angebots-Seite und dem (möglicherweise) folgendem Umsatz in Verbindung gebracht werden.
- Die Publisher-Seite erhält ggf. eine positive Argumentation für den Vertrieb von Werbeplätzen.

Dabei muss kritisch betrachtet werden, dass die ausspielenden Werbenetzwerke nicht nur eine oder zwei Newsseiten bestücken, sondern mit einer Vielzahl von Dienstleitungs-Anbietern als Content- und Werbemittel-Lieferant verbunden sind (vgl. Abb. 2). Basierend auf der großen Anzahl von Cookie-Daten entsteht ein gigantischer Pool an Informationen. Die Werbenetzwerke haben dadurch die Möglichkeit, vieler User über einen längeren Zeitraum und über mehrere Webangebote hinweg (Serverübergreifende Sitzungen) beobachten zu können, um detaillierte Nutzerprofile anzulegen.

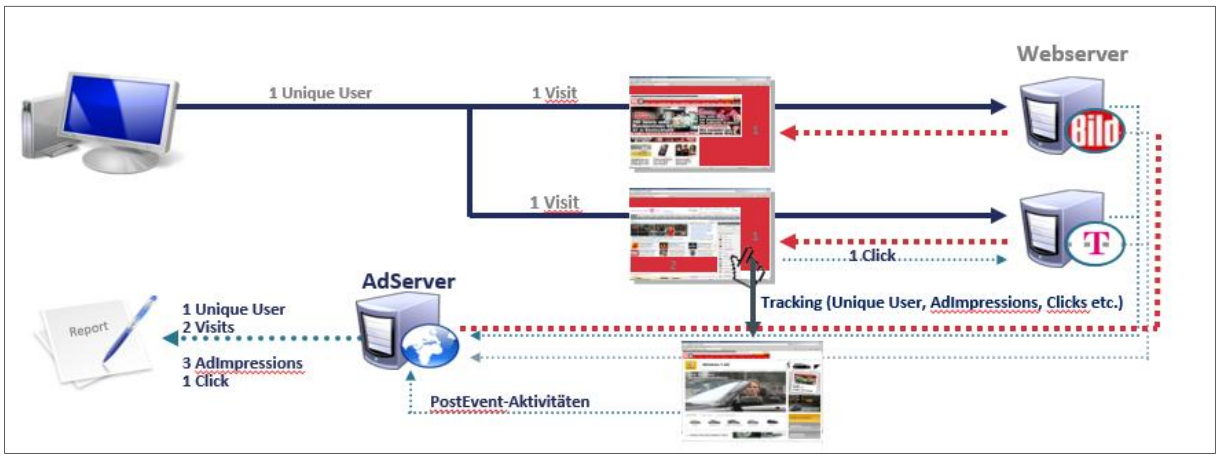

Abb.2: Darstellung der komplexen Vernetzungen zwischen Client, Webservern und Adserver

Es gibt eine große Anzahl an Add-ons oder Software Erweiterungen, die dem Anwender beim Surfen auf diese versteckten Tracker hinweisen und teilweise auch auf Wunsch blockieren. Die bekanntesten heißen „Lightbeam“ (bis 2013 Collusion) und Ghostery. Sehr plakativ hat das Global Editor Network[9] 2014 unter dem Projekt-Namen “The News read us”[10] dargestellt, wie viele externe „Mitleser“ auf souveränen Nachrichten-Seiten implementiert sind (vgl. Abb.3). Um dem Interesse der Werbetreibenden an dem Website-Publikum gerecht zu werden, zur Analyse und Optimierung ihrer Angebote oder auch um den sozialen Netzwerken eine einfache gemeinsame Nutzung von Inhalten zu ermöglichen, enthalten praktisch alle News-Sites eine große Anzahl von externen Tracking Beacons.

Abb.3: Visuelle Darstellung der Daten-Tracker auf spiegel.de

Bemerkenswert bei dem genannten Projekt ist neben der Analyse der Verbindungen zwischen den Nachrichtenseiten und den Tracking-Partnern, die ergänzende Darstellung der Datenhändler. Denn oft bündeln einige große Datenbanken eine Vielzahl an Tracking-Tools. Bei spiegel.de laufen 33 Tracker mit, die wiederum zu 23 Datenhändlern gehören.

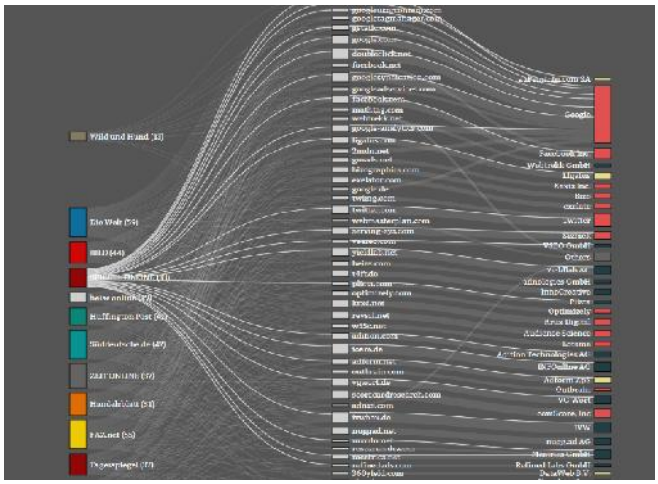

Abb.4: Vernetzte Strukturen von Tracking-Tools und Datenhändler

[9] **Global Editors Network**. [Online] 15. 01 2016. http://www.globaleditorsnetwork.org/editorslab/

[10] **Wehrmeyer, Stefan, Church, Annabel und Lindenberg, Friedrich**. News reads us. [Online] Made at the GEN Editor's Lab Berlin , 2014. [Zitat vom: 12. 01 2016.] http://newsreadsus.okfn.de/

Klassische Cookies sind dadurch charakterisiert, dass der Nutzer diese mehr oder weniger persönlich und einfach verwalten kann. Zum einen mit direkten Software-Einstellungen am Endgerät, durch Einsatz externer Software oder Add-ons zur Kontrolle von Cookies. Damit sollte ursprünglich die Hoheit über den Umgang mit persönlichen Daten gewährt werden.

4 Persistant Cookies

Wie im vorigen Artikel beschrieben, können klassische Cookies von Nutzern verwaltet und gelöscht werden. Um dies zu verhindern, haben Datensammler Alternativen entwickelt um einen permanenten Datentransfer zwischen Client und Server zu gewährleisten.

4.1 Evercookies

2010 veröffentlichte Samy Kamkar[11] die erste Version der Evercookies als open source und erfand damit ein (fast) unlöschbares Cookie. Evercookies setzen sich im DOM-Storage des Browser fest und können sich nach einem Löschversuch reanimieren. Diese Tracking-Cookies kombinieren unterschiedliche Techniken, um dem Nutzer persistent erhalten zubleiben. Es wird die herkömmliche HTTP Speicher-Technik genutzt und diese um weitere HTML5 Techniken ergänzt. Wenn der Cookie nun auf seinem bekannten Platz über die Software-Einstellungen „Cookies löschen“ entfernt wird, können die Daten aus den noch verfügbaren Informationen ein erneutes Cookie generieren. Nur wenn alle Speicherorte gleichzeitig gelöscht werden, könnte der Cookie eliminiert werden.
Eine Forschungsgruppe[12] der englischen Princeton University und der belgischen Katholieke Universiteit haben belegt, wie häufig diese Technik schon implementiert ist. Von den 100.000 größten Internet-Websites (gemäß AlexaRanking) verwenden bereits 107 Seiten die selbstwiederherstellenden Evercookies.

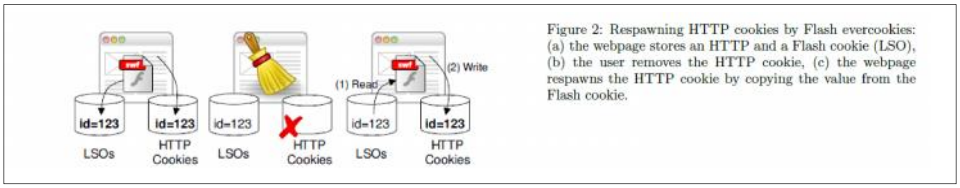

Figure 2: Respawning HTTP cookies by Flash evercookies: (a) the webpage stores an HTTP and a Flash cookie (LSO), (b) the user removes the HTTP cookie, (c) the webpage respawns the HTTP cookie by copying the value from the Flash cookie.

Abb.5: Funktionsweise eines Evercookies

[11] **Samy, Kamkar**. evercookie -- never forget. [Online] 20. 09 2010. [Zitat vom: 15. 01 2016.] http://samy.pl/evercookie/

[12] **Acar, Gunes, et al., et al.** The Web Never Forgets: Persistent Tracking Mechanisms in the Wild. s.l. : KU Leuven, Princeton University. ACM 978-1-4503-2957-6/14/11

4.2 Canvas Fingerprinting

Eine weitere Methode des Daten-Trackings, das der Nutzer kaum selbst verwalten kann, beschreibt das Canvas Fingerprinting. Dabei werden die Browser-Einstellungen ausgelesen und der Effekt ausgenutzt, das bei Canvas Elementen die Darstellung von Text, Sprache, Browser, Grafikkarte und Grafiktreiber sowie installierte Fonts bei jedem Nutzer variieren. Diese Unterschiede sind oft so subtil, dass sie dem Nutzer nicht auffallen. Dennoch sind sie so individuell, dass es anhand dieser Informationen möglich ist, über 90 Prozent der Internetnutzer wiederzuerkennen.[13]. Bei dem Besuch einer Webseite, wird dem Browser ein kleiner Text zum Auslesen der Einstellungen mitgegeben – dies geschieht häufig durch eingebundene Materialien wie Werbeplatzierungen, Social Media Buttons oder Bilder. Von diesem Zeitpunkt an, kann die einzigartige Darstellung der Seite mit dem Nutzer in Verbindung gebracht werden und der User wiedererkannt werden. Diese Daten können solange genutzt werden, wie der gleiche Browser mit seinen Einstellungen genutzt wird.
Im Zusammenhang mit der Electronic Frontier Foundation Studie, wurde auch ein Tool angelegt, das es ermöglicht zu sehen, welche Fingerprint Daten jeder User abgibt. Demnach hat nur ein weiterer Browser von bereits 793.412.625 Website-Besuchern den identischen „Fingerabdruck" meiner Browser-Einstellungen (vgl. Abb. 6). Bereits 2014[14] haben 5% der Top 100.000 Webseiten (weltweit) diese Art der Wiedererkennung genutzt bzw. zugelassen, daß Dritte diese Informationen generieren.

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
Limited supercookie test	0.83	1.77	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	N/A	N/A	6347c8[illegible]0740c202
Screen Size and Color Depth	7.47	177.16	1536x864x24
Browser Plugin Details	3.17	9.01	undefined
Time Zone	2.65	6.28	-60
DNT Header Enabled?	N/A	N/A	True
HTTP_ACCEPT Headers	N/A	N/A	text/html, */*; q=0.01 gzip, deflate de DE
Hash of WebGL fingerprint	N/A	N/A	[illegible]
Language	N/A	N/A	de DE
System Fonts	N/A	N/A	Arial, Arial Black, Arial Narrow, Arial Rounded MT Bold, Arial Unicode MS, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century, Century Gothic, Century Schoolbook, Comic Sans MS, Consolas, Courier, Courier New, Garamond, Georgia, Helvetica, Impact, Lucida Bright, Lucida Calligraphy, Lucida Console, Lucida Fax, Lucida Handwriting, Lucida Sans, Lucida Sans Typewriter, Lucida Sans Unicode, Microsoft Sans Serif, Monotype Corsiva, MS Gothic, MS Outlook, MS PGothic, MS Reference Sans Serif, MS Sans Serif, MS Serif, Palatino Linotype, Segoe Print, Segoe Script, Segoe UI, Segoe UI Light, Segoe UI Semibold, Segoe UI Symbol, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings, Wingdings 2, Wingdings 3 (via javascript)
Platform	N/A	N/A	Win32
User Agent	7.83	226.83	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Touch Support	N/A	N/A	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.42	1.34	Yes

Abb.6: Kriterien zur Fingerprinting Bestimmung

[13] **Peter, Eckersley**. How Unique Is Your Web Browser? s.l. : Electronic Frontier Foundation, 2014
[14] **Acar, Gunes, et al., et al.** The Web Never Forgets: Persistent Tracking Mechanisms in the Wild. s.l. : KU Leuven, Princeton University. ACM 978-1-4503-2957-6/14/11

5 Bedeutung für die Werbeindustrie

Für eine höhere Relevanz der Werbebotschaften beim Konsumenten und der damit einhergehenden Steigerung der Effizienz eingesetzter Werbemittel, strebt die Werbeindustrie persönlich zugeschnittene Angebotskommunikation an. Dieser Ansatz basiert auf der These, dass relevante Anzeigen einen höheren Impact haben und eine größere Reaktion erzielen. Um möglichst personalisierte Werbung schalten zu können, müssen Werbetreibende mehr über den User wissen: Was ihn interessiert, wo er sich aufhält, welche soziodemografischen Merkmale er aufweist, mit welchen Themen er sich beschäftigt, wohin er in den Urlaub fliegt und wer seine Freunde sind, um nur einige relevante Informationen zu nennen. Dafür wurden „Data Management Platforms“ (kurz: DMPs) entwickelt, die Nutzerdaten sammeln, kategorisieren und Muster erstellen. Oft liegen diese DMPs in den Händen großer Werbenetzwerke, die wie im Vorfeld beschrieben, durch ihre weitreichende Verbreitung auf einen riesigen Datenpool zugreifen können.

Aktuell etabliert sich in der digitalen Werbebranche der programmatische Einkauf. Der programmatische Handel bringt Werbetreibende mit ihrem Werbemittel mit relevanten Zielgruppen auf einer Internetseite (Inventar) im Auktionsverfahren zueinander. Öffnet ein User eine Content-Seite, so wird durch den AdServer ein Werbemittel platziert (vgl. Abb. 2). Doch bevor der AdServer dieses ausspielt, wird die Platzierung zur Auktion freigegeben. Den Zuschlag erhält der Werbetreibende, dem dieser Nutzer am meisten Wert ist. Die Entscheidung wird über maschinelle Entscheidungssysteme getroffen, denen meist Logarithmen zu Grunde liegen. Folgende Überlegungen werden in Bruchteilen von Sekunden während des Bietverfahrens angestellt:

- Stimmen die Nutzer-Daten mit unseren Zielgruppen-Kriterien überein?
- Hatte der User bereits Kontakt mit dem Werbemittel oder mit anderen Seiten des Unternehmens?
- Wie viele Informationen haben wir bereits vorliegen?
- Ist es ein aktiver User? Auf welche Anzeige hat er schon einmal reagiert?
- Mit welchen Themen beschäftigt er sich gerade?
- Wie sind die Erfahrungen mit der Content-Seite?
- Welche Werbemittel haben wir vorliegen und welches soll eingebaut werden?

Die implementierten Algorithmen versuchen anhand der vorliegenden Informationen eine Erfolgswahrscheinlichkeit zu errechnen, die einen Preis für diese Werbeplatzierung rechtfertigt. Anhand dieser Kalkulation wird ein Gebot abgegeben.

Der programmatische Werbemittelhandel wird auch in Deutschland schon bald den klassischen Vertriebsweg dominieren. In Anbetracht dieser Entwicklung haben User Daten als wichtigstes Bewertungskriterium schon heute eine zentrale, wirtschaftliche Relevanz.

6 Fazit

Millionenfach wird tagtäglich ein breites Spektrum an digitalen Spuren im World Wide Web gesammelt. Wenn man sich vor Augen führt, wie eindeutig das „Fingerprinting“ ist und wie „anhänglich“ Cookies sein können, kann von einer Anonymität im Netz nicht mehr gesprochen werden. Auch wenn diese Daten anonymisiert erhoben werden, ist es kein großer Schritt, auch noch den Namen zuzuordnen. Die technische Möglichkeit besteht bereits, generierte Daten mit persönlichen Informationen zu kombinieren, wie sie durch Log in Daten, Benutzerkonten oder Buchungstools abgegeben werden. Die Ursache dieser Daten-Sammel-Euphorie kann nicht allein bei den Seitenbetreibern gesucht werden. Der Treiber für diese rasante Entwicklung ist auch bei den beauftragten Werbedienstleistern zu suchen.

Besonders kritisch muss die Monopolisierung der Datenhändler beobachtet werden. Momentan läuft es darauf hinaus, dass einige wenige Unternehmen den Tracking-Markt kontrollieren und den Großteil aller Daten beherrschen werden. Die Firma AddThis stellt für Webseitenanbieter eine Software-Lösung zur Verfügung, mit dem die Seiten-Inhalte direkt in Social-Media-Diensten wie Twitter, Facebook oder Instagram geteilt werden können. Über diesen Weg hat AddThis bereits 1,7 Milliarden Browserinformationen gesammelt. [15] Seinen Umsatz generiert AddThis dann mit dem Verkauf dieser Nutzerprofile an Werbetreibende. Noch prägnanter wird dieser Zustand der Daten-Monopolisten am Beispiel von Google. Der ABC Konzern verteilt seine Datenquellen über tausende von Seiten; Search, Gmail, Drive, YouTube, Google Now, Play-Store, Nest, AdWords, DoubleClick oder Analytics, um nur einige zu nennen. Diese Datendichte erlaubt eine sehr genaue und tiefgreifende Analyse des Nutzers.

[15] Do not track. [Online] 2015. [Zitat vom: 20. 02 2016.] https://blog.donottrack-doc.com/de/t3n-magazin-wann-wer-wo-warum-online-tracking-muss-transparenter-werden/

Abschließend sollte jedem User bewusst sein, dass wir nicht „ungesehen“ im Internet agieren. Es ist möglich, Datenspuren Browser-, Geräte- und Plattformübergreifend nachzuverfolgen und zu detaillierten Nutzerprofilen zusammenzuführen – und dann jeder erkennen würde, dass wir ein Hund sind (vgl. Abb.7).

Abb.7: Peter Steiner's cartoon

7 Literatur- & Quellenverzeichnis

1. **Mackenzie, Joel, Choudhury, Farhana M. und Culpepper, J. Shane.** Efficient Location-Aware Web Search. s.l. : School of Computer Science and Information Technology, RMIT University, Australia, 2015. ACM 978-1-4503-4040-3/15/12.

2. **Aleyasen, Amirhossein, et al.** On the Privacy Practices of Just Plain Sites. Denver, Colorado, USA : s.n., 2015. ACM 978-1-4503-3820-2/15/10.

3. **live-counter.com.** [Online] [Zitat vom: 17. 02 2016.] http://www.live-counter.com/google-suchen/.

4. Vigneriy, Luigi , et al. Taming the Android AppStore: Lightweight. s.l. : EURECOM, Technicolor Research, 2015. Research Report RR-15-305.

5. Wolfie, Christl. FAZ.net. Facebooks Datenauswertung - Verstecken kann sich niemand mehr. [Online] 28. 04 2015. [Zitat vom: 06. 01 2016.] http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/facebooktracktseinenutzeronlineundoffline13562350p2..

6. Brendan, van Alsenoy, et al. From social media service to advertising network. [The ACM Digital Library]. s.l. : Interdisciplinary Centre for Law and ICT/Centre for Intellectual Property Rights of KU Leuven, the department of Studies on Media, Information and Telecommunication of the Vrije Universiteit Brussel, 2015.

7. Maps, Google. The official blog for Google Maps. [Online] 20. 05 2015. [Zitat vom: 12. 02 2016.] http://google-latlong.blogspot.de/2015/05/dont-let-traffic-slow-you-down-this.html.

8. Wikipedia. [Online] 05. 01 2016. https://de.wikipedia.org/wiki/HTTP-Cooki**e.**

9. Felten, Ed. Freedom to Tinker. [Online] 07. 07 2009. [Zitat vom: 12. 01 2016.] https://freedom-to-tinker.com/blog/felten/if-youre-going-track-me-please-use-cookies/.

10. Englehardt, Steven, et al. Cookies That Give You Away:. Florence : International World Wide Web Conference Committee, 2015. ACM 978-1-4503-3469-3/15/05.

11. Wehrmeyer, Stefan, Church, Annabel und Lindenberg, Friedrich. News reads us. [Online] Made at the GEN Editor's Lab Berlin , 2014. [Zitat vom: 12. 01 2016.] http://newsreadsus.okfn.de/.

12. Balabeko, Rebecca, et al. Measuring the Effectiveness of Privacy Tools for Limiting Behavioral Advertising. s.l. : Carnegie Mellon University, 2012. ACM 978-1-4503-1532-6.

13. Global Editors Network. [Online] 15. 01 2016. http://www.globaleditorsnetwork.org/editorslab/.

14. Samy, Kamkar. evercookie -- never forget. [Online] 20. 09 2010. [Zitat vom: 15. 01 2016.] http://samy.pl/evercookie/.

15. Acar, Gunes, et al. The Web Never Forgets: Persistent Tracking Mechanisms in the Wild. s.l. : KU Leuven, Princeton University. ACM 978-1-4503-2957-6/14/11.

16. Peter, Eckersley. How Unique Is Your Web Browser? s.l. : Electronic Frontier Foundation, 2014.

17. Do not track. [Online] 2015. [Zitat vom: 20. 02 2016.] https://blog.donottrack-doc.com/de/t3n-magazin-wann-wer-wo-warum-online-tracking-muss-transparenter-werden/.

8 Abbildungsverzeichnis

Versicherung über Selbstständigkeit

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

Hamburg, 29.02.2016

Ort, Datum

Unterschrift

Matrikel-Nr. 2252474