Gefällt mir, gefällt mir nicht – Tracking im Internet

Charlotte Röttgen, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Westfälische Wilhelms-Universität Münster*

1 Webtracking – eine Begriffserklärung

Nicht selten macht sich beim Surfen im Internet Verwunderung darüber breit, dass die eingeblendete Werbung ausgerechnet ebenjene Produkte bewirbt, für die man sich bereits seit Längerem interessiert. Wie kommt diese Verknüpfung von Informationen zustande, die sich beispielsweise in Form von „targeted advertising" (zielgruppenspezifische Werbung) offenbart? Die Antwort lautet: Durch Webtracking.

Mit Hilfe des Webtracking (deutsch: Nachverfolgung) erfahren Websitebetreiber unter anderem, wie lange sich ein User auf der Seite aufhält, von welcher Seite er auf diese zugegriffen hat, welche Aktivitäten er auf der Seite vornimmt und wie häufig er diese aufruft (Bouhs 2014). Ferner können Standortinformationen sowie Inhalte von E-Mail-Kommunikation getrackt werden. Durch die Auswertung dieser Vielzahl an Datenspuren, die ein User hinterlässt, kann der Verwender der Tracking-Technik Profile erstellen, die anhand von Wahrscheinlichkeiten Aussagen treffen über Interessen, politische Einstellung, den Bildungsgrad und sogar die sexuelle Orientierung der Websitebesucher. Diese Informationen sind geldwert, da sie eine zielgruppengenaue Werbung ermöglichen.

Allgemein gilt: Je mehr man über den Kunden, seine Interessen und Wünsche weiß, desto genauer können die Werbeinhalte auf ihn abgestimmt werden und umso höher ist die Wahrscheinlichkeit, dass er das beworbene Produkt kauft.

Auf einen Blick: Tracking im Internet

- Webtracking gibt es in verschiedenen Erscheinungsformen: Getrackt wird beispielsweise durch Cookies, die Einbettung eigener Inhalte auf Websites Dritter, Canvas Fingerprinting u.v.m.
- Die Einbettung von Social Plugins auf Webseites Dritter führt zu einer Vernetzung der verschiedenen Webcontent-Anbieter und einer Erweiterung des Tracking.
- Der *Datr-Cookie* von Facebook – verknüpft mit Social Plugins – sammelt auch Informationen von Nicht-Mitgliedern.
- Ein vollständiger Schutz vor Tracking ist nicht möglich; durch Browsereinstellungen für Cookies, deren manuelle Löschung sowie die Installation von AdBlockern kann Webtracking aber erschwert beziehungsweise eingeschränkt werden.
- Der EuGH entscheidet bald über die Frage, ob IP-Adressen Personenbezug haben oder nicht. Dies ist auch für die datenschutzrechtliche Beurteilung des Webtracking von Bedeutung.
- Anknüpfend daran wird auch der Personenbezug von Cookies und Canvas Fingerprints zu diskutieren sein.

2 Welche Arten des Webtracking gibt es?

Webtracking gibt es in verschiedenen Erscheinungsformen. Aufgrund der Vielzahl an Methoden sollen nachfolgend einige beispielhaft dargestellt werden.

Ein klassisches Tracking-Tool sind Cookies, kleine Textdateien, die im Browser des Websitebesuchers gespeichert werden und die Informationen über seinen Weg zu der Website – etwa über ein Werbebanner – und die Häufigkeit der Seitenaufrufe und das Surfverhalten auf der Website enthalten (Mauerer 2015: 26).

Es gibt unterschiedliche Arten von Cookies und nicht allen ist mit Misstrauen zu begegnen. Was sie alle gemeinsam haben, ist die Wiedererkennung eines Browsers respektive des Users. Entscheidend ist, von wem der Cookie stammt, der im Browser platziert wird und welche Intention damit verfolgt wird.

*Für seine wertvollen fachlichen Anmerkungen danke ich meinem Kollegen Nils Wehkamp.

Der von einem Websitebetreiber beim Aufrufen seiner Website im Browser gespeicherte Cookie (**Standard-Cookie**) dient primär der Vereinfachung des Websiteaufrufs (Mauerer 2015: 26). So ermöglicht die durch den jeweiligen Cookie garantierte Wiedererkennung ein schnelleres Laden der Website und macht, im Falle authentifizierungsbedürftiger Websites, ein erneutes Anmelden obsolet. Cookies von Drittanbietern hingegen ermöglichen ein websiteübergreifendes Tracking auf all jenen Websites, auf denen sie platziert sind (Cross-Site Tracking) (Schallaböck 2014[a]: 21; Schneider/Enzmann/Stopczynski 2014: 7).

Sog. **Zombie-Cookies** sind eine hartnäckige Variante der Tracking-Cookies, die sich nicht ohne weiteres vollständig löschen lassen. Der Cookie wird mehrfach und auf verschiedene Arten im Browser gespeichert. Wird er an einer Stelle gelöscht, wird dies erkannt und es erfolgt eine sofortige Wiederherstellung.

Eine weitere Maßnahme, welche in der Regel ergänzend neben den Tracking-Cookies verwendet wird, ist das Einbetten eigener Inhalte auf fremden Internetseiten durch **Social Plugins** (Lotz 2015: 199) von Facebook, Twitter, Tumblr oder Pinterest. Indem Facebook beispielweise den „Like-Button" auf diversen Websites platziert, kann das Unternehmen in Kombination mit der Nutzung von Cookies das Nutzerverhalten nachvollziehen (sog. Reichweitenanalyse) – selbst nachdem User die Facebook-Seite längst verlassen oder diese zuvor gar nicht aufgerufen haben.

Auch über die **IP-Adresse,** die bei jedem Aufruf einer Website mitgesendet wird, kann der Nutzer wiedererkannt werden und eine Geolokalisierung erfolgen (Lotz 2015: 196 f.). Eine ungefähre Standortermittlung ist möglich, da für bestimmte Regionen in der Regel bestimmte IP-Adressen vergeben werden (Schallaböck 2014[b]; Schultzki-Haddouti 2015).

Ein weiteres Tracking-Tool ist das **Canvas Fingerprinting**. Dieses ermöglicht es den Website-Betreibern, den digitalen Fingerabdruck des Nutzers auszulesen, indem über den Browser des Nutzers zahlreiche Konfigurationsdaten des abrufenden Gerätes (Browser-Version, Plugins, Betriebssystem, Bildschirmauflösung u.v.m.) übersendet werden (Mauerer 2015: 27). In Kombination mit weiteren Informationen lässt sich auch hierüber ein umfangreiches Profil erstellen.

Inhalte von E-Mails können auf bestimmte Signalwörter hin analysiert werden, um Interessen und Bedürfnisse des jeweiligen Nutzers zu erfassen und so gezieltere Werbung schalten zu können, sog. **E-Mail Tracking**. Von dieser Methode sind beispielsweise Nutzer mit einem Gmail-Account betroffen (Schallaböck 2014[b]).

Die Etablierung von Smartphones und Tablets hat dem Webtracking auf eine neue Ebene der Nutzeranalyse verholfen. Durch **App-Tracking,** ist eine anwendungsübergreifende Identifizierung der Nutzer möglich (Schneider, Enzmann & Stopczynski 2014: 53; Schallaböck 2014[b]; Schonschek 2014). Je nachdem, welche Apps auf dem Gerät vorhanden sind und welche Konfigurationen der Nutzer vorgenommen hat (oder auch nicht), werden neben dem Surfverhalten auch Standortdaten etc. aufgezeichnet. Häufig sind es „Gratis-Apps", die, unabhängig von dem angebotenen Dienst, Standortdaten aufzeichnen und eine weitreichende Analyse ermöglichen. Dass es sich in diesen Fällen um kostenlose Dienste handelt, also solche, die keiner Gegenleistung bedürfen, darf bezweifelt werden. Der Nutzer „zahlt" durch die Preisgabe seiner Daten.

Eine Methode aus dem Bereich der Verhaltensanalyse, die noch in den Kinderschuhen steckt, ist das **Tracking über die Tastatur** des jeweiligen Gerätes, mit dem der Nutzer im Internet surft (Datenschutzbeauftragter-Info 2015). Mithilfe spezieller Software[1], welche Eingabegeschwindigkeit, Tastendruck und Schreibverhalten des Nutzers analysiert, ist es möglich, Nutzer zu identifizieren. Laut Aussage des Unternehmens BehavioSec seien hierdurch in einer Testphase 99 Prozent aller Testpersonen erkannt worden (Olsen 2014).

Für die Unternehmen, welche die oben dargestellten Tracking-Tools vielfach kombiniert auf ihren Websites verwenden, kann die Reichweite der Nutzerverfolgung erheblich erweitert werden. Eine größere Reichweite erhöht nicht nur die Quantität der gesammelten Daten, mit denen Nutzerprofile gespeist werden können, sondern – dies ist ein entscheidender Punkt – auch die Datenqualität. Hierdurch ergibt sich schließlich ein ganzheitliches Mosaik des jeweiligen Nutzers.

[1]Unternehmen wie bspw. KeyTrack oder BehavioSec stellen Software her, die anhand des Tippverhaltens der Nutzer diese wiedererkennen kann.

3 Wie kann man verhindern, getrackt zu werden?

Es gibt verschiedene Möglichkeiten, Tracking einzugrenzen – vollständig verhindern lässt es sich jedoch nicht.

Der User hat über seine **Browsereinstellungen**, die manuelle **Löschung der Cookies** oder spezieller Browser-**Add-ons** wie beispielsweise AdBlock oder Ghostery die Möglichkeit, sich des Tracking zu erwehren.

In den neuesten Browser-Versionen ist, wenn man im Privaten Modus surft, ein **Trackingschutz** bereits vorinstalliert. Durch diesen werden sämtliche auf einer Blocklist des Browsers befindlichen Tracker blockiert (Horizont 2015).

Erwähnenswert ist auch der Ansatz des deutschen Unternehmens eBlocker, Webtracking durch den Einsatz von **Hardware** unmittelbar am WLAN-Router zu verhindern. Die Besonderheit ist, dass diese Anti-Tracking-Technologie sämtlichen Geräten Schutz bietet, die im WLAN-Netz eingeloggt sind.

Auch das **Abschalten der Javaskript-Funktion** stellt eine Möglichkeit dar zu verhindern, dass Cookies im Browser gespeichert werden, beziehungsweise zumindest die Anzahl der Cookies zu reduzieren. Diese Funktion ist in den neueren Versionen der gängigen Browser allerdings nur noch teilweise und nur durch Browser-Add-ons möglich.

Ein Nachteil solcher Schutzvorkehrungen ist jedoch, dass viele Seiten nicht mehr oder nur noch eingeschränkt nutzbar sind.

4. Das Beispiel Facebook

Am Beispiel der Social Media-Plattform Facebook soll die Verzahnung verschiedener Tracking-Methoden, insbesondere von Cookies und Social Plugins, veranschaulicht sowie die datenschutzrechtliche Brisanz der angewendeten Methoden aufgezeigt werden.

Die Webtracking-Praxis bei Facebook erfolgt durch die Implementierung des „Like-Buttons“ auf diversen Websites und den Einsatz von Cookies – insbesondere des *Datr-Cookies*, über den sich seit Jahren die Gemüter von Datenschützern erhitzen (vgl. Karg & Thomsen 2012: 729 f.; Süddeutsche 2015; ULD 2011: 23 f.).

Dieser Cookie ist mit dem „Like-Button“ von Facebook verknüpft und wird im Browser sämtlicher User gespeichert, die Websites aufrufen, auf denen der Button platziert ist. Hierbei kommt es nicht darauf an, ob der „Like-Button“ überhaupt betätigt wurde oder – und dies ist in datenschutzrechtlicher Hinsicht besonders brisant – der User überhaupt registriertes Facebook-Mitglied ist (Acar et al. 2015: 5 ff.). Dies ermöglicht bei jedem Aufruf einer Website mit implementiertem „Like-Button“ oder von Facebook-Fanpages[2] eine Wiedererkennung des Users über den zuvor in seinem Browser platzierten Cookie.[3] Darüber hinaus wird immer auch offengelegt, welche Websites von dem jeweiligen User zuvor besucht wurden.

Die Tatsache, dass auch Nicht-Mitglieder, die keine datenschutzrechtliche Einwilligung gegeben haben, von den Tracking-Technologien des Facebook-Konzerns erfasst werden, hat in jüngerer Vergangenheit die belgische und nun auch die französische Datenschutzbehörde zum Handeln bewogen. Nach geltendem EU-Recht ist eine datenschutzrechtliche Einwilligungserklärung[4] in diesen Fällen des Webtracking erforderlich.

Ende 2015 betrieb die belgische Datenschutzbehörde ein Gerichtsverfahren gegen Facebook (Belgian Privacy Commission 2015). Sie forderte Facebook auf, das oben beschriebene Vorgehen zu unterlassen und drohte eine Geldstrafe in Höhe von 250.000 € für jeden Tag an, an dem Facebook dieses – nach Ansicht der Datenschutzbehörde – datenschutzwidrige Verhalten fortsetzte. In erster Instanz erging ein obsiegendes Urteil, gegen das Facebook Berufung eingelegt hat (Gibbs 2016).[5]

In Frankreich setzte die Datenschutzaufsicht dem Unternehmen eine dreimonatige Frist, um die Überwachung von Nicht-Mitgliedern ohne deren Einwilligung zu

[2] Facebook-Fanpages sind frei zugänglich und werden häufig von Unternehmen, Vereinen, Institutionen, Personen der Öffentlichkeit etc. erstellt und dienen, den Auftritt über eine Homepage ergänzend oder diese ersetzend, dazu, User über sich zu informieren und mit ihnen in Kontakt zu treten.

[3] Nach dem Report der Belgischen Datenschutzbehörde wurde der Datr-Cookie nur dann im Browser von Nicht-Mitgliedern gespeichert, wenn diese eine Facebook-URL aufriefen. Erst danach konnte eine Verknüpfung über die Social Plugins erfolgen.

[4] Diese Regelungen sind im deutschen Recht in den §§ 4, 4a BDSG zu finden.

[5] Im Berufungsverfahren wurde die Klage der Datenschutzbehörde inzwischen mit der Begründung abgewiesen, Belgien sei nicht befugt, die Unternehmenspraxis von Facebook zu regeln, da dieses seinen Europäischen Hauptsitz in Irland und nicht in Belgien hat.

beenden (Untersinger 2016; Süddeutsche Zeitung 2016).

Für die Frage nach der datenschutzrechtlichen Zulässigkeit des Webtracking ist entscheidend, ob es sich bei den getrackten Informationen um **personenbezogene Daten** im Sinne des Bundesdatenschutzgesetzes handelt. Über den Personenbezug von IP-Adressen besteht seit Langem Streit in der Rechtswissenschaft und der Rechtsprechung (vgl. BGH 2011: 345; Schaar 2002: Kap. 3, Rn. 153; Eckhardt 2011: 339 f.; Hoeren, 2011: 4). Diese Frage hat der BGH im Jahr 2015 dem EuGH zur Klärung vorgelegt (Schleipfer 2015: 399 f.). Seine Entscheidung könnte weitreichende Folgen für die datenschutzrechtliche Beurteilung der gängigen Trackingpraxis haben.[6] In seinem Schlussantrag im Mai 2016 bewertete der Generalanwalt des EuGH *Sánchez-Bordona* (2016) IP-Adressen als personenbezogene Daten. Ob der EuGH dieser Einschätzung folgen wird, ist noch unklar.

5 Zusammenfassung und Ausblick

Die oben exemplarisch dargestellten Tracking-Verfahren offenbaren, dass die These, Daten seien das neue Öl, nicht von ungefähr kommt. Im Hinblick auf das kommerzielle Interesse der Beteiligten (Website-Anbieter, Marketingbranche und Unternehmen) verwundert es nicht, dass die Platzierung von Werbung Dritter auf einer Website für zahlreiche Website-Betreiber eine nicht unerhebliche Einnahmequelle darstellt. Die wachsende Tendenz der Internetnutzer, durch Adblocker und ähnliche Schutzmechanismen Werbung zu unterdrücken und das Tracking zu verhindern, ist zu dieser Praxis diametral.

Bereits jetzt zeichnet es sich ab, dass die Internetbranche hierauf reagieren und neue Methoden entwickeln wird, um das wirtschaftliche Potenzial auch zukünftig ausschöpfen zu können.

Die größte Tageszeitung Deutschlands beispielsweise reagierte dergestalt, dass ihre Website für Browser mit aktiviertem Adblocker nicht mehr zugänglich ist. Wer in den Genuss kostenlosen Contents kommen möchte, solle zumindest in Form von Werbung „zahlen". Zahlreiche Zeitungen haben sich bereits angeschlossen, weitere werden höchstwahrscheinlich folgen. Welche technischen Entwicklungen uns noch bevorstehen und wie Gesetzgeber und Rechtsprechung darauf reagieren werden, wird die Zukunft zeigen.

[6] In seinem Schlussantrag im Mai 2016 (Rechtssache C-582/14) bewertete Generalanwalt des EuGH *Sánchez-Bordona* IP-Adressen als personenbezogene Daten. Ob der EuGH dieser Einschätzung folgen wird, ist noch unklar.

Vertiefungshinweise

- Jan Schallaböck, 2014, Verbraucher-Tracking – Kurzgutachten
- ULD 2011, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf
- Do Not Track, Interaktive Webdoku-Reihe des BR. http://www.br.de/fernsehen/bayerisches-fernsehen/inhalt/film-und-serie/do-not-track-brett-gaylor-transmediales-projekt100.html

ABIDA (Assessing Big Data) Über die Dossiers

Das Projekt ABIDA, gefördert vom Bundesministerium für Bildung und Forschung, lotet gesellschaftliche Chancen und Risiken der Erzeugung, Verknüpfung und Auswertung großer Datenmengen aus und entwirft Handlungsoptionen für Politik, Forschung und Entwicklung. Dabei nähert ABIDA sich dem Thema Big Data aus einer grundlegend interdisziplinären Perspektive. Mehr Informationen finden Sie auf www.abida.de.
In den ABIDA-Dossiers werden regelmäßig ausgewählte Big Data-Themen kurz und prägnant dargestellt, um dem Leser einen Überblick zu liefern und einen Einstieg in die Thematik zu ermöglichen. Weitere Dossiers sind verfügbar unter www.abida.de/content/dossiers.

Literaturnachweise

Acar, G., v. Alsenoy, B., Piessens, F., Diaz, C., Preneel, B. (2015). Facebook Tracking Through Social Plug-ins, Technical Report for the Belgian Privacy Commission. Online verfügbar unter: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf.

Ansorge, K., Pimpl, R. (2015). Online advertising is rife with mistrust. Interview, Horizont.net. Online verfügbar unter: http://www.horizont.net/medien/nachrichten/Mozilla-Online-advertising-is-rife-with-mistrust-137450.

Belgian Privacy Commission (2015). The judgement in the Facebook case. Online verfügbar unter: https://www.privacycommission.be/en/news/judgment-facebook-case.

BGH (2015). EuGH-Vorlage zur Speicherung von dynamischen IP-Adressen – IP-Adressen. *Gewerblicher Rechtschutz und Urheberrecht, 192-196.*

BGH (2011) Speicherung dynamischer IP-Adressen. *Multimedia und Recht, 341-364.*

Bouhs, D. (2014). Der gläserne Internetnutzer. Deutschladfunk.de. Online verfügbar unter: http://www.deutschlandfunk.de/datenerfassung-der-glaeserne-internetnutzer.761.de.html?dram:article_id=293516

Datenschutzbeauftragter-Info.de (2015). Neue Tracking-Methoden: Tastatur-Eingaben und Akku-Ladestand. Online verfügbar unter: https://www.datenschutzbeauftragter-info.de/neue-tracking-methoden-tastatur-eingaben-und-akku-ladestand/.

Eckhardt, J. (2011). IP-Adresse als personenbezogenes Datum – neues Öl ins Feuer. *Computer und Recht 2011, 339-344.*

Gibbs, S. (2016). Facebook wins appeal against Belgian privacy watchdog over tracking, TheGuardian.com. Online verfügbar unter: https://www.theguardian.com/technology/2016/jun/30/facebook-wins-appeal-against-belgian-privacy-watchdog-over-tracking.

Hoeren, T. (2011). Google Analytics - datenschutzrechtlich unbedenklich?. *Zeitschrift für Datenschutz, 3-6.*

Karg, M., Thomsen, S. (2012). Tracking und Analyse durch Facebook – das Ende der Unschuld. *Datenschutz und Datensicherheit, 729-736.*

Lotz, P. (2015). E- Commerce und Datenschutzrecht im Konflikt. HMD Best Paper Award 2015, 192-202.

Mauerer, T. (2015). Web Privacy, Seminar Future Internet, Network Architectures and Services, 25-32. Online verfügbar unter: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2015-09-1/NET-2015-09-1_04.pdf.

Olsen, P. (2014). Forget Passwords. Now Banks Can Track Your Typing Behavior On Phones. Online verfügbar unter: http://www.forbes.com/sites/parmyolson/2014/08/18/forget-passwords-now-banks-can-track-your-typing-behavior-on-phones/#7ec1215c44cc.

Schaar, P. (2002). Datenschutz im Internet, 2002. München: C.H. Beck.

Sánchez-Bordona, M. C. (2016). Schlussantrag des Generalanwalts v. 12.05.2016, Rechtssache C-582/14. Online verfügbar unter: http://curia.europa.eu/juris/document/document.jsf?docid=178241&doclang=DE.

Schallaböck, J. (2014[a]). Verbraucher-Tracking, Kurzgutachten, iRights.Law. Online verfügbar unter: http://www.gruene-bundestag.de/fileadmin/media/gruenebundestag_de/themen_az/digitale_buergerrechte/Tracking-Bilder/Verbraucher_Tracking.pdf.

Schallaböck, J. (2014[b]). Was ist und wie funktioniert Webtracking? Online verfügbar unter: https://irights.info/artikel/was-ist-und-wie-funktioniert-webtracking/23386.

Schleipfer, S. (2015). Datenschutzkonformer Umgang mit Nutzungsprofilen. *Zeitschrift für Datenschutz*, 399-405.

Schneider, M.,Enzmann, M., Stopczynski, M. (2014). Web-Tracking-Report 2014, Fraunhofer SIT, Stuttgart 2014. Online verfügbar unter: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2014.pdf.

Schonschek, O. (2014). App-Tracking: Was Apps alles verraten, Datenschutz-Praxis.de. Online verfügbar unter: https://www.datenschutz-praxis.de/fachartikel/app-tracking-apps-alles-verraten/

Schultzki-Haddouti, C. (2015). Ein bisschen Datenschutz ist schon eingebaut. FAZ.de. Online verfügbar unter: http://www.faz.net/aktuell/technik-motor/computer-internet/privatsphaere-und-tracking-ein-bisschen-datenschutz-ist-schon-eingebaut-13838753.html.

Sueddeutsche.de (2015). Datenschützer: Facebook hat keinen Respekt vor Privatsphäre. Online verfügbar unter:http://www.sueddeutsche.de/digital/tracking-datenschuetzer-facebook-hat-keinen-respekt-vor-privatsphaere-1.2483240.

Sueddeutsche.de (2016). Französische Datenschützer werfen Facebook Gesetzesverstöße vor. Online verfügbar unter: http://www.sueddeutsche.de/news/service/internet-franzoesische-datenschuetzer-werfen-facebook-gesetzesverstoesse-vor-dpa.urn-newsml-dpa-com-20090101-160209-99-585875.

Unabhängiges Landeszentrum für Datenschutz (2011). Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook. Online verfügbar unter: https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf.

Untersinger, M. (2016). Données personnelles: levirulent réquisitoire de la CNIL contre Facebook, LeMonde.fr. Online verfügbar unter: http://www.lemonde.fr/pixels/article/2016/02/09/donnees-personnelles-le-virulent-requisitoire-de-la-cnil-contre-facebook_4861621_4408996.html.