International Working Group
on Data Protection
in Telecommunications

675.46.18

Arbeitspapier

Webtracking und Privatsphäre:

Die Beachtung von Kontext, Transparenz und Kontrolle bleibt unverzichtbar

53. Sitzung, 15. – 16. April 2013, Prag (Tschechische Republik)

- Übersetzung -

Einleitung

1. Dieses Papier gründet auf der Achtung der Grundrechte und Grundfreiheiten der Internetnutzer. Obgleich der Fokus nicht auf besonderen technischen Maßnahmen liegt, geht das Papier gleichwohl davon aus, dass das technische Verfahren des Webtracking rechtmäßig und angemessen sein und dass es sich innerhalb eines strengen Rahmens dieser Rechte bewegen muss. Die Grundsätze von Wahlmöglichkeiten und Kontrolle – die von großen Teilen der Wirtschaft gefordert werden – bilden das Zentrum dieses Rahmens; diese Grundsätze müssen mit Genauigkeit auf den Säulen von Klarheit, Transparenz und Verantwortlichkeit umgesetzt werden. Die Rechtfertigung für die Durchführung von Webtracking ist nicht offenkundig, deshalb müssen die Wirtschaft und andere Vertreter, die Tracking durchführen, beständig nach Lösungen suchen, die diese Tätigkeit nicht nur voll und ganz in den Rahmen der Grundrechte und Privatsphäre einpassen, sondern sie auch mit dem Gebot des „Privacy by Design“ *[Einbeziehung des Schutzes der Privatsphäre schon bei der Entwicklung von Technologien]* in Einklang bringen.

2. In diesem Arbeitspapier behandelt die Arbeitsgruppe das Thema Webtracking und Privatsphäre. Obgleich es keine klare Definition dafür gibt, werden wir uns auf eine Definition des Webtracking[1] beziehen, nämlich als der Erhebung, Analyse und Anwendung von Daten über Nutzeraktivitäten von einem Computer oder Gerät aus, wenn verschiedene Dienste der Informationsgesellschaft (nachfolgend: das Internet)[2] genutzt werden, um diese Nutzungsdaten zu verschiedenen Zwecken

[1] van Eijk (2012), The DNA of OBA: unique identifiers *[Die DNA der OBA: Eindeutige Identifikatoren] [OBA = Online Behavioural Advertising = Online-Werbung mit Nutzung des Surfverhaltens der Nutzer]*, URL: http://www.campusdenhaag.nl/crk/publicaties/robvaneijk.html#definition-of-web-tracking .

[2] Beachten Sie bitte, dass dadurch, dass die Technologie auf IP-Grundlage zunehmend zum Rückgrat der Informationsgesellschaft wird und viele andere früher eigenständige Technologien integriert wurden(„Konvergenz”), dies auch die Nutzung von Telefon (IP-Telefonie) und Fernsehen (IPTV), das Lesen digitaler Zeitungen oder jeglicher anderer Medienkonsum mittels digitaler Technologien (einschließlich das Lesen eines E-Buches) mit umfassen kann. Zu einer detaillierten Diskussion der sich daraus ergebenden Gefahren für die Privatsphäre siehe das Working Paper „Privacy Issues in the

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

zusammen zu führen und zu analysieren, und zwar von wohltätigen und philantropischen bis hin zu kommerziellen Zwecken. Wir sind der Meinung, dass verschiedene Formen der Marktforschung unter diese Definition des Webtracking fallen, zum Beispiel die Reichweitenmessung („outreach measurement" – der Umfang, in dem Nutzer Anzeigen überall im Internet angezeigt bekommen), das Messen des Nutzungsverhaltens („engagement measurement" –der Umfang, in dem Nutzer mit Internetdiensten in Interaktion treten) und das Messen der erreichten Nutzer („audience measurement" – der Umfang, in dem Mikroprofile der Nutzer aus ihrer Interaktion mit Angeboten im Internet abgeleitet werden können).[3]

Distribution of Digital Media Content and Digital Television *[Arbeitspapier zu Themen der Privatsphäre bei der Verbreitung digitaler Medieninhalte und des digitalen Fernsehens]* (Berlin, 4./5.09.2007) dieser Gruppe; URL: http://www.datenschutz-berlin.de/attachments/349/digit_de.pdf.

[3] JICWEBS Reporting Standards *[Grundsätze der Berichterstattung im Internet des Joint Industry Committee for Webstandards]*, URL: http://www.abc.org.uk/PageFiles/50/Web Traffic Audit Rules and Guidance Notes version2 March 2013 master.pdf .

Umfang des Arbeitspapiers

3. Dieses Papier richtet sich an alle Anbieter von Web-Sites sowie an Softwareentwickler und Service Provider *[Diensteanbieter]*, die Trackingtechnologien anbieten oder nutzen. Dieses Papier diskutiert die Entwicklung von Trackingtechnologien und ihre möglichen Auswirkungen auf die Privatsphäre der Bürgerinnen und Bürger. Es befasst sich mit digitalen Spuren, die wir hinterlassen, wenn wir die verschiedenen Dienste der Informationsgesellschaft mit einem Webbrowser nutzen, dazu gehören auch eindeutige Identifikatoren („unique identifier"), die mit Hilfe von Technologien erlangt werden, die ohne Cookies arbeiten.[4] Dazu zählen ferner auch Webbrowser auf anderen Geräten, zum Beispiel auf Smartphones und Smart-TV-Geräten.

4. Dieses Papier befasst sich nicht mit besonderen zusätzlichen Gefahren der Nutzung von Apps auf mobilen Geräten.[5] Nichtsdestotrotz sollten die Grundsätze dieses Papiers ebenso auf in anderen Diensten eingesetzte Trackingmethoden angewandt werden.

5. In diesem Papier geht es nicht darum, wie Schutzmaßnahmen umgesetzt werden können (z.B. rechtliche Anforderungen an eine Einwilligung). Anzumerken ist jedoch, dass in manchen Rechtsordnungen zwar je nach Zweck des Webtracking, die ausdrückliche Einwilligung (Opt-in) erforderlich ist, in anderen Rechtsordnungen jedoch die Möglichkeit zum Widerspruch („Opt-Out") für das Webtracking als gültig betrachtet wird, um den Anforderungen des Rechtssystems zu genügen, wenn bestimmte Bedingungen erfüllt sind. Diese umfassen unter anderem die angemessene Benachrichtigung über die Verarbeitung von Daten; Transparenz in der Benachrichtigung; Benachrichtigung zum Zeitpunkt der Sammlung der Daten oder zuvor; und einfache, wirksame und dauerhafte Möglichkeiten zum Widerspruch. Eine Reihe von Beschränkungen kann ebenso vorhanden sein; z.B. in Bezug auf die Verarbeitung sensibler Informationen wie zum Beispiel Informationen über die Gesundheit, über politische oder weltanschauliche Ansichten und die Verhinderung des Tracking von Kindern.

Hintergrund

6. Die technischen Möglichkeiten für die Beobachtung der Aktivitäten der Nutzer auf Web-Sites haben sich in den letzten zehn Jahren vervielfältigt; die „Informationsgesellschaft" hat seitdem schon mehrere grundlegende Veränderungen erfahren.[6] Webtracking entwickelte sich aus sehr

---

[4] Zum Beispiel die passive Fingerprinting-Technik, die auf dem Hashing des HTTP Endsystemteils bzw. der IP-Adresse des Ursprungs-Browsers basiert.

[5] Siehe zum Beispiel die von der Artikel-29-Datenschutzgruppe (Art. 29 WP) herausgegebene Stellungnahme 02/2013 über Apps auf Smart-Geräten WP 202, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf .

[6] Die Literaturübersicht über die Messung der Privatsphäre im Internet, welche als Ergebnis der Konferenz zur Messung der Privatsphäre im Internet (Conference on Web Privacy Measurement, WPM) zusammengestellt wurde, gibt einen ausführlicheren Überblick über die für das Tracking eingesetzten Technologien, URL: http://www.law.berkeley.edu/12633.htm .

bescheidenen Anfängen – als einzelne Provider von Online-Diensten mit der Beobachtung ihrer Nutzer mit dem Ziel der Feststellung begannen, ob ein bestimmter Nutzer diese Web-Site schon zuvor besucht hatte und was dieser Nutzer dort getan hatte – in jüngerer Zeit zu einer schon fast bizarren Vision der Anbieter. In dieser Vision scheint der Anbieter in der Lage zu sein, jeden einzelnen Aspekt des Verhaltens eines erkennbaren Nutzers im gesamten Internet zu beobachten. Dies könnte eine vollständige Verlaufsübersicht über die umfassende Nutzung des Internets einer betroffenen Person über unbegrenzte Zeitspannen hinweg (wortwörtlich von der Wiege bis zum Grab) werden, und diese *[Verlaufsübersicht]* könnte mit Profildaten aus der „Offline-Welt" angereichert werden (einschließlich aller möglichen Aspekte aus unserem Leben, über die die Datenmakler Informationen besitzen; dazu gehören auch Informationen über Finanzen sowie Informationen über zum Beispiel Freizeitgestaltung, Gesundheit, politische bzw. religiöse Überzeugungen und Informationen über Aufenthaltsorte).[7]

7. Diese Entwicklung – die zwar von Anbietern und anderen Interessenten in der Geschäftswelt begrüßt und gefördert und von einigen Politikern auf nationaler und regionaler Ebene unterstützt wird – birgt eine beispiellose Gefahr für die Privatsphäre aller Bürger in der Informationsgesellschaft. Sie könnte schlimmstenfalls die uns bekannte Welt zu einem globalen Panoptikum wandeln: Das Offline-Äquivalent wäre, wenn uns ein Unbekannter ständig über die Schulter schauen würde, ganz gleich, wo wir uns befinden (auf der Straße oder in der scheinbaren Privatsphäre zu Hause) – oder was wir gerade tun (fernsehen, online einkaufen, Zeitung lesen und sogar noch intimere Tätigkeiten) und ohne dass wir wissen, wann der Unbekannte gerade zuschaut und wann nicht.[8]

8. Die möglichen Auswirkungen einer solchen Entwicklung liegen auf der Hand und sind im Hinblick auf ihre mögliche Schwere nicht zu unterschätzen: Sie kann einige der wesentlichen Grundsätze der Privatsphäre aufheben oder anullieren, – und insbesondere *[die Grundsätze von]* Transparenz und Kontrolle durch die Bürgerinnen und Bürger.[9] Um es noch deutlicher zu sagen: Dies könnte das Ende der Welt (in Bezug auf den Schutz der Privatsphäre) sein, wie wir sie kennen.

9. Die Befürworter dieser Vision behaupten andererseits, dass diese Gefahren entweder gar nicht vorhanden sind oder dass sie versucht haben, sich mit diesen Gefahren zu befassen und sie zumindest zum Teil abzuschwächen: Es gibt einen starken Widerstand seitens mancher Interessenvertreter der Wirtschaft dagegen, anzuerkennen, dass eindeutige Identifikatoren Daten über die Internetnutzung personenbezogene Informationen sind. Eine oftmals vorgebrachte Behauptung ist, dass bei vielen der genutzten Daten die Rückverfolgung auf eine bestimmte Person nicht mehr möglich ist (d.h. die Daten anonymisiert wurden) und dass, sobald dieses erledigt ist, die Daten sich nicht mehr auf eine Person beziehen und deshalb keine Gefahr mehr für die Privatsphäre von Bürgern darstellen würden. Auch wird vorgebracht, dass alle Daten über Verhaltensweisen nur mit Maschinen verbunden sind und – dies ist die Behauptung – in sehr vielen Fällen überhaupt nicht zu einer bestimmten Person zurückverfolgt werden können.

---

[7] In Systemen zur Pflege der Kundenbeziehungen (Customer Relationship Management, CRM) sind hierfür die üblichen Begriffe Customer Lifetime *[Kundenleben]* und Customer Lifetime Value *[Kundenkapitalwert]*.

[8] Und um die Dinge noch zu verschlimmern, würde diese modernistische Version eines Panoptikums jede einzelne Bewegung einer jeglichen Privatperson und zu einem jeden Augenblick aufzeichnen, unabhängig davon, ob der Wächter gerade hinschaut oder nicht.

[9] Tracking als Technologie ist nicht transparent: Auf technischer Ebene sind in vielen Fällen die Pixel *[Bildpunkte]* (z.B. Web-Beacons *[Code-Fragmente]*) und Mini-Web-Sites (z.B. iFrames) für das menschliche Auge unsichtbar.

10. Allerdings gibt es für diese Behauptungen keinerlei wissenschaftlichen Nachweis und sie lassen die Tatsache außer Acht, dass Maschinen – und insbesondere Smartphones – zunehmend zu persönlichen Geräten werden und eine Verbindung zu einem jeden individuellen Nutzer leicht ermöglichen. Spuren können auch in zunehmendem Maße über verschiedene Geräten hinweg verbunden werden. Ebenso gibt es einen wissenschaftlichen Nachweis dafür, dass viele anscheinend anonyme Daten (z.B. Informationen über den Aufenthaltsort bei Mobiltelefonen) zu dem betroffenen Nutzer zurückverfolgt werden können (d.h. ihre Anonymisierung wird aufgehoben), wenn die Datenbasis und der zeitliche Rahmen groß genug sind. Jüngere wissenschaftliche Arbeiten lassen sogar vermuten, dass es grundsätzlich unmöglich ist, „anonyme" Daten vor einer Deanonymisierung zu schützen, wenn der Zeitintervall für die Beschreibung eines beliebigen Verhaltens groß genug ist (d.h. es ist schon konzeptuell unmöglich, zu garantieren, dass „anonyme" Daten im Laufe der Zeit nicht zu einer bestimmte Person zurückverfolgt werden können). Wenn dies richtig ist, stellt es eine bahnbrechende Entwicklung dar und würde eine Reihe von Kernannahmen darüber, wie sich die Nutzung verschiedener Arten von Daten auf die Privatsphäre von Personen auswirken kann oder nicht, sinnlos machen. [10]

11. Darüber hinaus und mit leicht anderer Ausrichtung trägt auch die praktische Erfahrung des Alltags dazu bei, die von der Industrie aufgestellten Behauptungen in Frage zu stellen: Werbeanzeigen werden zwar auf technischer Ebene an eine Maschine gerichtet, es ist aber nicht die Maschine, die letzten Endes die sprichwörtlichen „schönen roten Schuhe" kauft – es ist der oder die Einzelperson. Deshalb kann die Behauptung, dass die Verarbeitung von Daten über Verhaltensweisen für Marketingzwecke sich „nur" zunächst an Maschinen richtet, sehr wohl als ein Versuch betrachtet werden, unseren Blick als Gesellschaft insgesamt hinsichtlich der Ernsthaftigkeit des Problems zu trüben, da in der Realität der Mensch und nicht die Maschine die einzige Instanz ist, die alle solche Trackingoperation zu einem „Erfolg" für die Befürworter gestalten kann (d.h., wenn die roten Schuhe schließlich gekauft werden).

[10] Cf. Ohm, Paul: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization *[Gebrochene Versprechen zur Privatsphäre: Eine Antwort auf das überraschende Versagen der Anonymisierung]*, August 2009. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 .

Eine kurze Geschichte der Technologien für Beobachtungszwecke

12. Bei dem Versuch, die oben beschriebene Entwicklung bis zu ihren bescheidenen Anfängen hin zurück zu verfolgen, stellt die Entwicklung der „Cookie-Technologie" vor fast 20 Jahren ein Meilenstein dar: HTTP-Cookies wurden 1994 eingeführt, und zwar in erster Linie, um das „kleine" Problem der verlässlichen Umsetzung eines virtuellen Einkaufswagens zu lösen. Weil das Hypertext Transfer Protocol (HTTP) überwiegend zustandslos („stateless") war, konnten Endsysteme bis zu diesem Zeitpunkt keine Zustandsinformationen speichern. Die Speicherung von Zustandsinformationen war jedoch für den virtuellen Einkaufswagen ganz wesentlich, um ausgewählte Artikel beim Shopping-Vorgang zu speichern. Transparenz war schon zu diesem Zeitpunkt ein Thema im Hinblick auf die Privatsphäre, weil die Verwendung von Cookies dem gewöhnlichen Nutzer nicht mitgeteilt wurde. Zu jener Zeit wurden Cookies standardmäßig in den Browsereinstellungen freigegeben und der Nutzer wurde über den Einsatz von Cookies nicht informiert.[11]

13. Um Gefahren für die Privatsphäre und die Sicherheit zu entschärfen, die sich daraus ergeben, dass Cookie-Informationen ungewollt zu Betreibern anderer Web-Sites gelangen, wurde die Same-Origin-Policy *[Grundregel desselben Ursprungs, SOP]* eingeführt. Diese Maßnahme bedeutet, dass Cookies nur von derselben Domain gelesen werden konnten, die sie gesetzt hat. Allerdings muss darauf hingewiesen werden, dass das World Wide Web Consortium (W3C) *[Gremium zur Standardisierung der das Internet betreffenden Techniken]* einen neuen Standard vorgeschlagen hat, nämlich das Cross Origin Resource Sharing (CORS)[12], welches den Informationsaustausch domainübergreifend zulässt. Obgleich CORS ein freiwilliger Standard ist, steht er im Widerspruch zur Same-Origin-Policy.

14. Bereits 1998 befasste sich diese Gruppe[13] mit verschiedenen Fragestellungen zur Privatsphäre in Verbindung mit der systematischen Sammlung oder Nutzung personenbezogener Daten im Internet.[14] In dem Arbeitspapier beschäftigte sie sich mit P3P (Platform for Privacy Preferences Project) *[Plattform zum Austausch von Datenschutzinformationen]*, einem vom W3C entwickelten Protokoll, welches darauf ausgelegt war, Cookies von Dritten zu blockieren, es sei denn, dass die vom Nutzer besuchte Web-Site eine für den Nutzer akzeptable P3P-Policy *[P3P-Datenschutzrichtlinie]* anbot.[15] Allerdings hat nur ein großer Browserhersteller den Standard umgesetzt. Infolgedessen wurde P3P in keinem breiten Umfang im Internet angenommen.

---

[11] RFC 2109, HTTP State Management Mechanism, URL: https://tools.ietf.org/html/rfc2109. Beachten Sie, dass aktuelle Varianten der Speichertechnik für Cookies zum Beispiel auch Flash-Cookies und LSOs (Local Shared Objects) umfassen, die in HTML5 mit entsprechenden Werten verwendet werden.

[12] Cross-Origin Resource Sharing, URL: http://www.w3.org/TR/cors/ (abgerufen am 30. Mai 2013).

[13] International Working Group on Data Protection in Telecommunications *[IWGDPT,Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation]*.

[14] Gemeinsamer Standpunkt zu grundlegenden Eigenschaften datenschutzfreundlicher Technologien (z. B. P3P) im WorldWideWeb; (Hong Kong, 15.04.1998), http://www.datenschutz-berlin.de/attachments/177/priv_de.pdf

[15] Das Platform for Privacy Preferences Project (P3P) ermöglicht Web-Sites, ihre jeweiligen Methoden für den Umgang mit Privatsphäre in einem Standardformat auszudrücken, das automatisch abgefragt und von Nutzeragenten *[Anwendungssoftware, z.B. browser]* leicht interpretiert werden kann. P3P Nutzeragenten ermöglichen den Nutzern, über Methoden der Web-Site Kenntnis zu erlangen (sowohl in maschinenlesbaren, als auch für Menschen lesbaren Formaten) und Entscheidungsprozesse gegebenenfalls auf der Grundlage dieser Methoden zu automatisieren. Nutzer müssen nicht auf jeder von ihnen besuchten Web-Site die Datenschutzrichtlinien lesen. URL: http://www.w3.org/P3P/ .

15. Third Party Cookies *[Cookies von Dritten]* sind zum Lebensnerv der komplexen digitalen Werbeindustrie geworden. 2008 diskutierten leitende Marketingfachleute aus Webtracking-Unternehmen die Zukunft von Webanalyse und Webstatistik. Die Zukunft in fünf Jahren stellte man sich so vor, dass die traditionelle Webstatistik über die Besuche der Web-Site (nachfolgend: First und Third Party Analytics) mit Analysedaten anderer Webanalysedienste zusammengeführt wird, zu denen auch zum Beispiel Videodienste, Widgets *[Komponenten von Benutzeroberflächen]*, soziale Netzwerke, Spiele und Suchmaschinen gehören (nachfolgend: Web Analytics).[16]

16. Heutzutage stellen Daten aus Webanalysen eine neue Form des wirtschaftlichen Wertes dar. Zwar stellt diese Gruppe nicht den Nutzen in Frage, den das Messen des Verbraucherverhaltens für das Online Behavioural Advertising (OBA) *[Online-Werbung mit Nutzung des Surfverhaltens der Nutzer]* (in Echtzeit) bringen kann, doch ist sie der festen Überzeugung, dass solche Methoden nicht auf Kosten der Rechte von Privatpersonen im Hinblick auf Privatsphäre und Datenschutz eingesetzt werden dürfen.

Webtracking

17. Das Webtracking umfasst die Erhebung und nachfolgende Speicherung, Nutzung oder den Austausch von Daten des individuellen Online-Verhaltens über eine Vielzahl von Web-Sites durch den Einsatz von Cookies, JavaScript oder jeglichen anderen Formen des Device Fingerprinting *[Ermittlung von Einzelpersonen anhand von Eigenschaften technischer Geräte, z.B. Browser-Einstellungen]*. Webtracking-Technologien ermöglichen einen konstanten Fluss von Informationen über Nutzer in Echtzeit, wie zum Beispiel Registrierungsdaten, Daten über die Online-Suche, verhaltensbezogene Daten, Statistiken über Besuche von Web-Sites und Conversion-Daten *[Daten über Umwandlung von Klicks in Handlungen, wie z.B. Einkäufe]*, die alle widerspiegeln, auf welche Art und Weise ein Nutzer auf individuelle Angebote reagiert hat. Diese Daten können genutzt werden, um auf die Interessen, politischen Überzeugungen oder Krankheiten eines Nutzers zu schließen. Sie können mit dem Ziel verarbeitet werden, den Zustand oder das Verhalten einer bestimmten Person einzuschätzen, beides auf eine bestimmte Art und Weise zu behandeln oder zu beeinflussen. Daten über individuelles Verhalten lenken geschäftliche Entscheidungen auf der Grundlage von Kundenprofilen. Eine Kaufabsicht kann aus der vermuteten digitalen Identität einer Person abgeleitet werden. Der Wert eines potenziellen Kunden wird mit der Möglichkeit in Verbindung gebracht, ihn zum Kauf einer Ware zu bringen.

18. Webtracking-Technologie ist auf mobilen Geräten vorhanden. Privatpersonen tauschen ein mobiles, „smartes“ Gerät untereinander sehr wahrscheinlich nicht aus, und daher ist die Verbindung zwischen dem Gerät und der Privatperson enger als zum Beispiel zwischen Mensch und Desktop-Computer. Mobile Geräte enthalten eindeutige Geräte-Identifikatoren, wie zum Beispiel besondere Identifikatoren für Werbung,[17] die Unique Device ID (UDID) *[eindeutige maschinenlesbare Kennung]*,

[16] Omma Global Measurement 3.0, http://www.webmetricsguru.com/archives/2008/09/measurement-30-on-the-next-5-years-omma-global-day-2/ .

[17] Um zum Beispiel Frequency Capping durchführen zu können (Kontrolle der Häufigkeit, wie oft einem Nutzer eine Anzeige von Online-Werbung eingeblendet wird), Behavioral Ads *[auf Surfverhalten beruhende Anzeigen]* einzublenden und die Reichweite und Wirksamkeit einer Werbeaktion zu messen.

die MAC-Adresse (Media Access Control) *[Hardware-Adresse z.B. jedes einzelnen Netzwerkadapters]*, die Bluetooth MAC-Adresse, die NFC MAC-Adresse (Near Field Communications) *[international genormter Standard zur Datenübertragung im Nahbereich]*, die International Mobile Subscriber Identifier (IMSI, eine eindeutige SIM-Kartennummer) und die International Mobile Equipment Identifier (IMEI) *[eindeutige Seriennummer bei Mobilgeräten]*. Diese Identifikatoren kann der gewöhnliche Nutzer nicht ändern. Über eindeutige Identifikatoren hinaus können mobile, „smarte" Geräte eine große Menge an Daten enthalten, wie zum Beispiel Nutzernamen, Passwort, Alter, Geschlecht und das Adressbuch. Solche Geräte können genaue verhaltensbezogene Daten über den Aufenthaltsort eines Nutzers offenlegen. Präzise Geopositionsdaten stehen für Browser auf mobilen, „smarten" Geräten fertig nutzbar zur Verfügung.

19. Webtracking-Technologie wird auf verschiedene Art und Weise eingesetzt. Eine digitale Datenspur kann sich aus der unabsichtlichen oder ungewollten Offenlegung von Daten ergeben und zu einer nicht erforderlichen Offenlegung (personenbezogener) Daten führen. Es gibt sehr viele verschiedene Wege zur Erzeugung einer digitalen Datenspur. Zum Beispiel könnte der Manager einer digitalen Anzeigenaktion dem Nutzer, Browser oder Gerät einen eindeutigen Identifikator zuordnen. Ein anderer Weg ist die Personalisierung von Verweisinformationen durch Hinzufügen von Zielgruppeninformationen (Mikroprofile) beim Surfen im Internet, sodass andere Web-Sites, die sich auch an der Werbeaktion beteiligen, den Nutzer, Browser oder das Gerät ebenso nachverfolgen können. Ein drittes Beispiel ist die Korrelation eindeutiger Identifikatoren mit aus früheren Besuchen auf einer bestimmten Web-Site gesammelten Daten. Und ein viertes Beispiel ist, dass Webtracking für eine Werbeaktion durch die Kombination neuer Trackingdaten (über einen Nutzer, einen Browser oder Gerätedaten) mit zuvor auf einer bestimmten Web-Site gesammelten Daten oder mit von einem anderen oder Dritten erhaltenen Daten stattfinden kann. Ein letztes Beispiel sieht die Nutzung von Cookie Matching-Services *[Dienste zum Abgleich von Cookies auf besuchten Web-Sites mit dem auf dem Computer des Nutzers abgelegten Cookie]* vor, welche digitale Spuren desselben Nutzers, Browsers oder Gerätes mit der Nutzung verschiedener Teile des Internets verbinden. [18]

20. Webtracking besteht aus mehreren automatisierten Schritten, beginnend mit der Erhebung von Daten über die Internet-Nutzung, der Speicherung dieser Daten und der Nutzung der Daten. Durch neue Zusammenstellung der Daten, Korrelation und ihre Dekontextualisierung können Internetdaten dazu genutzt werden, sehr detailgenaue Profile und Vorhersagen individuellen Verhaltens aufzubauen. Schließlich führt das Webtracking zur tatsächlichen Anwendung des Profils einer bestimmten Person.

21. Daten können mittels verschiedener Dienste im Internet in einer Graphen-Ddatenbank gespeichert werden.[19] Die Struktur des Graphen ermöglicht die Herausbildung von Verhaltensmustern, die sonst unentdeckt geblieben wären. Webtracking-Daten in einem Graphen können aus sich selbst heraus oder durch Kombination mit anderen Daten aus verschiedenen Quellen aussagekräftige Muster über das Nutzerverhalten generieren. Zum Beispiel geben einzelne eindeutige Identifikatoren, die direkt

[18] Siehe zum Beispiel URL: https://developers.google.com/ad-exchange/rtb/cookie-guide#what-is .

[19] Ein Graph basiert auf der Graphentheorie, die einen mathematischen Ansatz für die Entwicklung paarweiser Beziehungen zwischen Objekten darstellt. Eine Graphdatenbank speichert Graphen, welche im wesentlichen Strukturen mit Knoten, Ecken und Eigenschaften darstellen. Die Eigenschaften können Metainformationen über die Knoten und Ecken enthalten.

oder indirekt mit einem Nutzer oder Computer verbunden sind, zwar nur wenige Informationen über den gelegentlichen Surfer bekannt, doch die Sammlung eindeutiger Identifikatoren bietet einen tief greifenden Einblick in die Gewohnheiten und das Surfverhalten einer Person im Internet. Die Sammlung eindeutiger Identifikatoren kann zur Erstellung einer digitalen Identität benutzt werden.

Webtracking und das Recht auf Privatsphäre und Datenschutz der Privatperson

22. Ein Schlüsselgrundsatz für eine große Bandbreite internationaler Rechtsordnungen ist das Recht auf Privatsphäre, das der Internetnutzer unabhängig von der Technologie besitzt. Schlüsselelemente sind Transparenz, Kontrolle und Beachtung des Kontextes. Es ist eine Gefahr für die Privatsphäre, dass Nutzern nicht bewusst ist, dass ihre Spuren verfolgt werden. Webtracking als Prozess verwendet eine Reihe technischer Tools, die die Gelegenheit der Mitteilung an die Nutzer begrenzen. Zum Beispiel sind Pixel (z.B. Web-Beacons) und Mini-Web-Sites (z.B. iFrames) für das menschliche Auge unsichtbar und ihre Einbindung in eine Web-Site löst eine automatische HTTP-Anfrage einschließlich der Möglichkeit des Setzens von und des Zugangs zu Cookies aus, die ihrerseits eindeutige Identifikatoren enthalten.

23. Viele Webtracking-Technologien wurden entwickelt und in der Wirtschaft eingesetzt, ohne dass den Nutzern Informationen darüber bereitgestellt wurden, wessen Daten gesammelt werden und ohne ihnen eine Wahlmöglichkeit zu bieten. Meldungen des Nutzers, die als Ausdruck der Ablehnung des Tracking verstanden werden könnten, wurden nicht beachtet und technische Methoden gegen einige Trackingmethoden wurden aktiv umgangen, zum Beispiel durch erneutes Hervorbringen gelöschter Cookies, (passives) Fingerprinting und das Umgehen von Browsereinstellungen. Erst als dieses Verhalten aufgedeckt und öffentlich kritisiert wurde, haben die entsprechenden Parteien ihre Verpflichtung akzeptiert, den freien Willen des Nutzers zu achten. In solchen Fällen wurden manchmal Opt-Out-Programme hinzugefügt, was aber oft zu schwerfälligen Mechanismen mit nur begrenztem Nutzen für den Nutzer führte. Diese Fälle haben im Hinblick auf das Vertrauen der Nutzer in die Verlässlichkeit und Aufrichtigkeit aller Internetanbieter einen großen Schaden verursacht und die gesunde Entwicklung innovativer Internetdienste untergraben.

24. Webtracking bedeutet in vielen Rechtsordnungen die Verarbeitung personenbezogener Daten, und zwar aufgrund der Tatsache, dass die Technologie die Individualisierung oder Identifizierung[20] von Nutzern bzw. das Treffen automatisierter Entscheidungen über sie ermöglicht. Ein Beispiel einer solchen Praxis könnten Maschinen für automatische Entscheidungen mit Algorithmen in Real Time Bidding Plattformen *[Verfahren für Werbungtreibende für das Bieten auf Werbeplätze in der Online-Werbung in Echtzeit]* für personalisierte Werbung auf der Grundlage von Nutzerverhalten sein.

25. Es gibt einen starken Widerstand seitens einiger beteiligter Interessengruppen gegen die Einstufung eindeutiger Identifikatoren in Webdaten als personenbezogene Informationen. Eine oftmals

[20] Erwägungsgrund Nr. 26 der allgemeinen Datenschutzrichtlinie 95/46/EG: Die Schutzprinzipien müssen für alle Informationen über eine bestimmte oder bestimmbare Person gelten. Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. *[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html]* (…), URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML .

vorgebrachte Behauptung ist die, dass sobald Daten anonymisiert wurden, [21] diese Daten nicht mehr personenbezogen sind. Es sollte jedoch klar sein, dass auch ein „zweckgebundenes" Element dafür verantwortlich sein kann, dass Informationen „sich" auf eine bestimmte Person „beziehen" oder diese Person betreffen können.[22]

Die potenzielle Wirkung (oder mangelnde Wirkung) des „Do Not Track" (DNT) *[nicht verfolgen]* – eine Fallstudie

26. Im September 2011 gründete das W3C die Tracking Protection Working Group[23] *[Arbeitsgruppe zum Schutz vor Webtracking]*. Die Gruppe arbeitet an einem Do-Not-Track Standard (DNT). Alle großen Browserhersteller haben sich zwar dazu verpflichtet, den Standard umzusetzen (und die meisten haben bereits den HTTP-Header umgesetzt), allerdings dauert bei jenen Interessengruppen, die den DNT:1 Request[24] beachten werden, eine offene Diskussion über Teile des freiwilligen Standards an. Einige Interessengruppen haben angedeutet, das DNT-Flag aus verschiedenen Gründen nicht beachten zu wollen. Der übergreifende Erfolg von DNT ist von der tatsächlichen Beachtung des DNT-Flag durch die empfangende Organisationen und der tatsächlichen Annahme des DNT-Standards im gesamten Internet durch alle Interessengruppen abhängig.

27. Standardeinstellungen im DNT und die Standardaktionen der Webtracking-Organisationen bleiben wiederum äußerst wichtig. Damit DNT ein wirksames Instrument für die Umsetzung der Kontrolle durch den Benutzer ist, ist es somit äußerst wichtig, dass die Betreiber von Webtracking auch sicher sein können, dass die von ihnen empfangene DNT-Meldung eine echte Anzeige der Wünsche des Nutzers darstellt. Fehlt dem Nutzer eine solche Wahlmöglichkeit mit umfassender Informationen, muss eine Webtracking-Organisation annehmen, dass einem Nutzer das Webtracking nicht bewusst ist, und deshalb muss sie dann von der Standardeinstellung ausgehen, als ob sie nämlich eine DNT:1 Meldung erhalten hätte, welches den Wunsch des Nutzers anzeigt, dass Tracking unerwünscht ist.

28. Jede für die Zwecke des Webtracking eingesetzte Technologie muss angemessen sein. Weltweit angewandte Datenschutzgrundsätze basieren auf der Vorstellung, dass Daten für spezifizierte, explizite und rechtmäßige Zwecke gesammelt und nicht auf eine Art und Weise weiterverarbeitet werden sollten, die mit solchen Zwecken unvereinbar ist. Die Verarbeitung von Daten sollte angemessen und relevant sein und nicht exzessiv im Verhältnis zu den Zwecken stehen, für die sie gesammelt bzw. weiterverarbeitet werden.

---

[21] De-Identifikation von Daten einer bestimmten Person bedeutet das Entfernen, Ändern, Kumulieren, Anonymisieren oder anderweitige Manipulation von Daten.

[22] Stellungnahme Nr. 4/2007 zum Begriff der personenbezogenen Daten (Arbeitspapier WP136), S. 10 URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf .

[23] Die Aufgabenstellung der Tracking Protection Working Group besteht darin, die Privatsphäre und Kontrolle durch die Nutzer zu verbessern, und zwar durch die Definition von Mechanismen zum Ausdruck von Festlegungen durch Nutzer rund um das Webtracking und zum Blocken oder Zulassen von Webtracking-Elementen, http://www.w3.org/2011/tracking-protection/charter .

[24] Im aktuellen Entwurf des DNT-Standards bedeutet das Aussenden von „0"-Meldungen das Einverständnis mit Tracking und „1" zeigt an, dass Tracking NICHT gewünscht wird.

29. Schließlich muss eine jede Technologie gerichtsfest sein, wenn sie dazu beitragen soll, dem Schutze der Privatsphäre zu dienen. DNT läuft Gefahr, ein Werkzeug zu bleiben, durch das ein Nutzer Wünsche gegenüber Serviceprovidern der Informationsgesellschaft ausdrücken kann, ohne dass dieses ein wirksames Instrument für einen konstruktiven Dialog darstellt. Dies lässt den Nutzer selbst oder eine jede öffentlich-rechtliche (oder private) Körperschaft, die mit die Durchsetzung solcher Wünsche oder Regelungen beauftragt ist (einschließlich der entsprechenden rechtlichen Verpflichtungen, die Auswahl einer Einzelperson zu beachten) im Hinblick auf solche Anbieter mit leeren Händen dastehen. Manche Interessenvertreter der Wirtschaft versuchen die Position zu verteidigen, dass das DNT keine Verpflichtung zur Beachtung eines Wunsches darstellt. Zwar ist diese Interpretation mehr als zweifelhaft, doch bleibt die Tatsache im Raume stehen, dass der Beweis schwer zu führen ist, ob ein solcher Wunsch beachtet oder missachtet wurde.[25] Mit anderen Worten, das DNT könnte aus der Perspektive der Umsetzung ein Placebo anstatt eines wirksamen Heilmittels bleiben, und als solches würde es auch nutzlos bleiben.

[25] Ein externes Audit könnte bei der Lösung von zumindest Teilen der oben beschriebenen Probleme eine wichtige Rolle spielen, würde aber andererseits das Ökosystem noch komplexer gestalten.

Empfehlungen

30. Ungeprüftes Webtracking kann das Gleichgewicht zwischen Dienstanbietern und Privatpersonen auch im Hinblick auf den Schutz der Privatsphäre verändern. Die Arbeitsgruppe unterstreicht, dass Kontext, Transparenz und Kontrolle äußerst wichtige Elemente auch im Kontext des Webtracking bleiben.

31. Um zur Lösung der Gefahren für die Privatsphäre der Privatperson beizutragen, gibt die Arbeitsgruppe die folgenden Empfehlungen an die verschiedenen Interessenvertreter, die im Ökosystem des Webtracking eine Rolle spielen.

Wiedereinführung der Beachtung von Kontext und Zweckbegrenzung als Kerngrundsätze für jede Nutzung personenbezogener Daten:

- Umsetzung von Vorsichtsmaßnahmen für jede (automatisierte) Erhebung, Verarbeitung und die Praxis des Austausches von Daten, sodass in einem bestimmten Kontext gesammelte Daten nicht in einem anderen Kontext angewandt werden können;

- Information über den Zweck der Erhebung von Daten gleich zu Beginn und im Vorhinein und keine Änderung des Zweckes ohne erneute Information und Wahlmöglichkeit.

Wiederherstellung der Transparenz:

- Keine Verwendung unsichtbarer Trackingelemente;

- Mindestens eine verständlich formulierte Mitteilung an den Nutzer, wenn das Anwendungsprogramm im Begriff ist, eine Webtracking-Kennzeichnung an den Empfangsserver zu senden oder eine solche Kennzeichnung vom Ursprungsserver zu empfangen;

- Einblenden einer für den Nutzer ausreichend erkennbaren Anzeige[26] immer dann, wenn Webtracking gerade stattfindet;

- Anzeige eines Hinweises, dass Webtracking gerade stattfindet, der auch für besondere Nutzergruppen, einschließlich der Sehbehinderten, zur Verfügung steht.

Rückverlagerung der Kontrollmöglichkeit zum Nutzer:

- Einrichtung von Mechanismen, die den Nutzern die Ausübung ihres Rechtes auf Privatsphäre und Datenschutz im Internet ermöglichen und kein Einsatz (neuer) Trackingmethoden, welche keine Kontrolle durch den Nutzer ermöglichen; Angebot der Möglichkeit zur expliziten Auswahl bezüglich

[26] Ein besonderes Augenmerk muss darauf gerichtet werden, sicherzustellen, dass keine Nutzergruppe des Internets benachteiligt oder anderweitig diskriminiert wird, zum Beispiel aufgrund einer Behinderung.

des Tracking an Nutzer - wenn Browsersoftware installiert, aktiviert oder aktualisiert wird, muss der Nutzer eine Wahlmöglichkeit besitzen;

- Besitzt der Browser keine Anwenderschnittstelle (user interface), sollte die Standardeinstellung so sein, dass das Tracking des Nutzers nicht stattfindet;

- Einräumen der Möglichkeit für Nutzer zur Änderung der Auswahl- und der Änderungseinstellungen nach der ursprünglichen Entscheidung und zu jeder Zeit; Schaffung einer einfachen Prüfmöglichkeit für den Nutzer für die (automatisierten) Wahlmöglichkeiten, die für das Webtracking getroffen wurden; Erinnerung des Nutzers daran, dass Wahlmöglichkeiten bezüglich der (automatisierten) Einstellungen für das Webtracking jederzeit widerrufen werden können und Sicherstellung, dass eine Änderung der Auswahl technisch auf einfache Art und Weise möglich ist, welche der Einzelperson keine ungebührliche Last auferlegt.

- Beachten von Mitteilungen, wenn das Anwendungprogramm meldet, dass Tracking abgelehnt wird;

- Unterlassung des (passiven) Fingerprinting, zum Beispiel durch Mining *[Durchsuchen]* der vom Nutzer generierten Daten (wie zum Beispiel Service Configurations oder User Agent Strings *[Zeichenkette, mit der sich der Browser identifiziert]*), um daraus eine eindeutige Benutzerkennung abzuleiten (Device Fingerprinting), wenn ein Nutzer mitgeteilt hat, dass er Tracking ablehnt.

- Sicherstellen, dass der Einsatz einer jeden Technologie mit dem Ziel, dem Nutzer Wahlmöglichkeiten zu geben, prüffähig ist und von den zuständigen, mit der Umsetzung von Bestimmungen beauftragten privaten oder öffentlich-rechtlichen Körperschaften auch überprüft werden kann, und insbesondere die Umsetzung der in den verschiedenen vorhandenen Rechtssystemen niedergelegten Bestimmungen, welche ihrerseits die Grundlage für den Schutz der Privatsphäre der Privatperson in vielen Rechtsordnungen weltweit bilden.