ARTIKEL-29-DATENSCHUTZGRUPPE

14/DE
WP 224

Stellungnahme 9/2014 zur Anwendung der Richtlinie 2002/58/EG auf die Nutzung des virtuellen Fingerabdrucks

Angenommen am 25. November 2014

Diese Arbeitsgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist das unabhängige Beratungsgremium der Europäischen Union in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG festgelegt.

Die Sekretariatsgeschäfte werden von der Europäischen Kommission, Generaldirektion Justiz, Direktion C (Grundrechte und Unionsbürgerschaft), B-1049 Brüssel, Belgien, Büro MO-59 02/013 wahrgenommen.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN,

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 und Artikel 30 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Zusammenfassung

Bei der Nutzung von virtuellen Fingerabdrücken gibt es ernsthafte Bedenken hinsichtlich des Schutzes personenbezogener Daten. Eine Reihe von Online-Diensten hat beispielsweise vorgeschlagen, als Alternative zu HTTP-Cookies den virtuellen Fingerabdruck für die Zwecke der Analyse oder des Tracking zu nutzen. Dies würde es ermöglichen, die in Artikel 5 Absatz 3 vorgesehene Einwilligung zu umgehen.[1] Dieses Beispiel zeigt, dass die vom virtuellen Fingerabdruck ausgehenden Risiken nicht theoretischer Natur sind. Forschungsergebnisse belegen zudem, dass der virtuelle Fingerabdruck bereits genutzt wird.[2]

In dieser Stellungnahme befasst sich die Artikel-29-Datenschutzgruppe mit der Problematik des virtuellen Fingerabdrucks und der Frage, ob Artikel 5 Absatz 3 der Richtlinie 2002/58/EG (e-Datenschutz-Richtlinie), geändert durch die Richtlinie 2009/136/EG, unbeschadet der Bestimmungen der Datenschutz-Richtlinie 95/46/EG auf die Nutzung des virtuellen Fingerabdrucks anwendbar ist. Die Kernaussage dieser Stellungnahme lautet, dass Artikel 5 Absatz 3 der e-Datenschutz-Richtlinie auf die Nutzung des virtuellen Fingerabdrucks anwendbar ist.

Diese Stellungnahme geht über die frühere Stellungnahme 04/2012 (Ausnahme von Cookies von der Einwilligungspflicht)[3] hinaus und weist Dritte[4], die virtuelle Fingerabdrücke verarbeiten, die beim Zugriff auf oder der Speicherung von Informationen auf dem Endgerät des Nutzers generiert wurden, darauf hin, dass dies nur mit der gültigen Einwilligung des Nutzers gestattet ist, sofern nicht eine Ausnahmeregelung gilt.

2. Einleitung

Nach Artikel 5 Absatz 3 der Richtlinie 2002/58/EG, geändert durch die Richtlinie 2009/136/EG[5] (e-Datenschutz-Richtlinie), stellen die Mitgliedstaaten 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*

[1] Wall Street Journal, 2013. Web Giants Threaten End to Cookie Tracking. http://online.wsj.com/news/articles/SB10001424052702304682504579157780178992984

[2] Nikiforakis, 2013. Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting. https://lirias.kuleuven.be/bitstream/123456789/393661/1/

[3] Artikel-29-Datenschutzgruppe, 2012. Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_de.pdf

[4] „Dritte“ im Sinne des Erwägungsgrundes 66 der Richtlinie 2009/136/EG.

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0136:de:NOT

von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG[6] *u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat".*[7]

In der Stellungnahme 04/2012 ging die Artikel-29-Datenschutzgruppe davon aus, dass es einen Zusammenhang zwischen Artikel 5 Absatz 3 der e-Datenschutz-Richtlinie und der Speicherung von Informationen oder dem Zugriff auf Informationen mit Hilfe von Cookies gibt. Der Stellungnahme zufolge ist Artikel 5 Absatz 3 nicht nur auf Cookies, sondern auch auf „vergleichbare Technologien" anwendbar.

Dieser Stellungnahme liegt eine wachsende Zahl von Berichten zugrunde, wonach Dritte aktiv technische Alternativen zu Cookies erforschen, die für vielfältige Zwecke eingesetzt werden können und die es ihnen ermöglichen, das Einwilligungserfordernis nach Artikel 5 Absatz 3 zu umgehen. Insbesondere wird die Kombination einer Reihe von Informationselementen untersucht, mit denen bestimmte Geräte oder Anwendungsinstanzen durch die Nutzung des virtuellen Fingerabdrucks („device fingerprinting") eindeutig identifiziert werden sollen.

Virtuelle Fingerabdrücke können auch personenbezogene Daten darstellen. Diese Stellungnahme enthält keine Analyse der einschlägigen Bestimmungen der Datenschutzrichtlinie, sondern bezieht sich auf Fragen des Datenschutzes, die im Zusammenhang mit dem virtuellen Fingerabdruck besonders relevant sind. Dies ist beispielsweise der Fall, wenn mehrere Informationselemente, vor allem eindeutige Kennungen wie IP-Adressen, miteinander kombiniert werden, und der Zweck der Verarbeitung darin besteht, Nutzer über Internetseiten zu identifizieren, beispielsweise mit Hilfe verhaltensorientierter Werbung. In solchen Fällen muss die Verarbeitung auch im Einklang mit den Bestimmungen der Datenschutzrichtlinie erfolgen.

Der virtuelle Fingerabdruck ist technologisch nicht auf die Konfigurationsparameter eines herkömmlichen Webbrowsers auf einem Desktop-PC beschränkt. Ebenso wenig ist er an ein bestimmtes Protokoll gebunden, sondern lässt sich zur Ermittlung des Fingerabdrucks von zahlreichen mit dem Internet vernetzten Geräten, von Unterhaltungselektronik und Anwendungen verwenden, auch solchen, die auf mobilen Geräten, intelligenten Fernsehern, Spielekonsolen, E-Buch-Lesern, Internetradios, fahrzeuginternen Systemen oder intelligenten Zählern laufen.[8]

3. Begriffsbestimmung

Ein Fingerabdruck ist gemäß RFC6973[9] als eine Reihe von Informationselementen zur Identifizierung eines Gerätes oder einer Anwendungsinstanz definiert. In dieser Stellungnahme wird der Begriff in einem weiteren Sinn verwendet und umfasst eine Reihe von Informationen, die dazu verwendet

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:NOT

[7] 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.

[8] Bisweilen als „Internet der Dinge" bezeichnet.

9 Cooper, 2013. Privacy Considerations for Internet Protocols. http://tools.ietf.org/html/rfc6973

werden können, im Zeitablauf einen Nutzer, einen Benutzeragenten oder Geräte herauszugreifen[10], zu verknüpfen[11] oder herzuleiten[12]. Dies umfasst beispielsweise Daten aus

(a) der Konfiguration eines Benutzeragenten (User Agent)/Gerätes oder

(b) durch die Verwendung von Netzwerkprotokollen zugängliche Daten.

Es gibt viele Arten von Daten, die einen Fingerabdruck bilden können, darunter

(a) CSS-Informationen;

(b) JavaScript-Objekte (z. B. Dokument, Fenster, Bildschirm, Browser, Datum und Sprache);

(c) HTTP-Kopfdaten (z. B. Zahl der Informationsbits in der Benutzeragenten-Zeichenfolge (User-Agent-String), Abfolge im HTTP-Header, Variationen des HTTP-Headers je nach Art der Abfrage);

(d) Uhrzeitinformationen (z. B. Uhrabweichung und Zeitfehler);

(e) Variation des TCP-Stapels;

(f) installierte Schriftarten;

(g) Informationen zu installierten Plug-ins (z. B. Angaben zu Konfiguration und Version);[13]

(h) Verwendung interner Programmierschnittstellen[14] (API), die über den Benutzeragenten/das Gerät zugänglich sind;

(i) Verwendung externer API von Webdiensten, mit denen der Benutzeragent/das Gerät kommuniziert.

---

[10] *Herausgreifen („singling out"):* Die Möglichkeit, in einem Datenbestand einige oder alle Datensätze zu isolieren, welche die Identifizierung einer Person ermöglichen; Stellungnahme 05/2014 zu Anonymisierungstechniken, S. 13

[11] *Verknüpfbarkeit („linkability"):* Die Fähigkeit, mindestens zwei Datensätze, welche dieselbe Person oder Personengruppe betreffen, zu verknüpfen (in derselben Datenbank oder in zwei verschiedenen Datenbanken). Ist ein Angreifer in der Lage (z. B. mittels Korrelationsanalyse) festzustellen, dass zwei Datensätze dieselbe Personengruppe betreffen, ohne jedoch einzelne Personen in dieser Gruppe herauszugreifen, bietet die betreffende Technik zwar einen Schutz vor dem „Herausgreifen", nicht aber vor der Verknüpfbarkeit; Stellungnahme 05/2014 zu Anonymisierungstechniken, S. 13.

[12] *Inferenz („inference"):* Die Möglichkeit, den Wert eines Merkmals mit einer signifikanten Wahrscheinlichkeit von den Werten einer Reihe anderer Merkmale abzuleiten; Stellungnahme 05/2014 zu Anonymisierungstechniken, S. 13.

[13] *Vgl.* a) http://www.w3.org/wiki/Fingerprinting, b) http://w3c.github.io/fingerprinting-guidance/#wsj-orbitz c) https://wiki.mozilla.org/Fingerprinting und d) https://trac.webkit.org/wiki/Fingerprinting für die Verfahren.

[14] Die API bietet einen nutzerfreundlichen Rahmen für den Zugang zu den Funktionen oder Routinen einer Software-Komponente.

4. Technischer Hintergrund

Bei der Entwicklung des Internets und des Webs wurden die Anforderungen einer widerstandsfähigen und offenen Netzwerk-Architektur berücksichtigt.[15] Aufgrund der konzeptionellen Entscheidungen zur Erfüllung dieser Anforderungen übermitteln Geräte Informationselemente. Eine Reihe von Protokollen umfasst zahlreiche obligatorische und fakultative Informationselemente. Beispielsweise enthält das HTTP/1.1[16]-Protokoll Header-Felder, die es Server und Client ermöglichen, zusätzliche Informationen über den Hypertext einzufügen. Einige hiervon sollen es dem Server ermöglichen, Client-Typen zu erkennen. Beispielsweise enthält der Anforderungsheader des Benutzeragenten folgende Beschreibung: „*Dies dient statistischen Zwecken, der Rückverfolgung von Protokollverletzungen, und der automatischen Erkennung von Benutzeragenten, um die Antworten so maßschneidern zu können, dass Beschränkungen bestimmter Benutzeragenten überwunden werden*".

Die Zeichenfolge des Benutzeragenten wird unter anderem verwendet, um das Layout des Inhalts für bestimmte Geräte zu optimieren, um Inhalte an bestimmte Nutzer zu richten[17], oder um aus Sicherheitsgründen oder zu Analysezwecken Informationen über das Gerät zu sammeln.

5. Datenschutzrisiken

Da ein einzelner HTTP-Header in der Regel einen nicht eindeutigen Wert enthält, können einzelne Nutzer nur selten allein aufgrund dieses Merkmals identifiziert werden.[18] Beispielsweise sind die von einem Browser unterstützten Medienarten häufig dieselben bei vielen anderen Nutzern, die die gleiche Browser-Version verwenden. Daher bilden diese nicht eindeutigen Merkmale bei isolierter Verarbeitung im Allgemeinen kein Datenschutzrisiko.

Mehrere Informationselemente können jedoch zu einem Datenpaket kombiniert werden, das hinreichend eindeutig ist (vor allem, wenn es mit weiteren Merkmalen wie der IP-Adresse kombiniert wird), um einen Fingerabdruck für das Gerät oder die Anwendungsinstanz zu ergeben. Aufgrund eines solchen Fingerabdrucks lässt sich ein Gerät von einem anderen unterscheiden, und der Fingerabdruck kann als verdeckte Alternative für Cookies zum Tracking von Internetverhalten verwendet werden.[19][20][21]Folglich kann eine Einzelperson mit diesem virtuellen Fingerabdruck verknüpft und somit identifiziert oder identifizierbar gemacht werden.

---

[15] Kahn, 1972. Communications Principles for Operating Systems. Internal BBN memorandum.

[16] Fielding, Reschke, 2014. Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. http://www.ietf.org/rfc/rfc7231.txt

[17] Wall Street Journal, 2012. On Orbitz, Mac Users Steered to Pricier Hotels, http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html

[18] Es kann jedoch in Fällen wie bei einem OAuth-Zugangstoken vorkommen, dass ein einziges Merkmal Informationen enthält, die die eindeutige Identifizierung einer einzelnen Person ermöglichen.

[19] Panopticlick, Electronic Frontier Foundation, 2010. https://panopticlick.eff.org/

[20] Yen, 2012. Host Fingerprinting and Tracking on the Web: Privacy and Security Implications. http://research.microsoft.com/pubs/156901/ndss2012.pdf

Die mit dem virtuellen Fingerabdruck verbundenen Datenschutzrisiken werden noch dadurch verschärft, dass eindeutige Datensätze nicht nur dem Betreiber einer Webpräsenz, sondern auch vielen anderen Dritten zugänglich sind. Dieser Umstand steht im Gegensatz zu der „Strategie des gleichen Ursprungs“ von HTTP-Cookies und wird durch den technischen Charakter des World Wide Web verstärkt, in dem viele Dritte zum Inhalt einer Webseite beitragen.

Es ist üblich, dass eine einzelne Webseite in Echtzeit unter Abrufe von Inhalten aus mehreren Quellen dynamisch erzeugt wird. Jede dieser Ressourcen generiert eigene HTTP-Abfragen und stößt das Herunterladen von Bildern, JavaScript- und CSS-Dateien an. Zahlreiche Webseiten enthalten außerdem Web-Bugs und Tracking-Skripte. Sie können zudem über HTTP-Abfragen aufzeichnen, wenn ein Nutzer auf Seiten, Bilder oder Werbung klickt oder diese auf dem Bildschirm verschiebt. Daher bietet sich Dritten häufig die Gelegenheit, die für die Ermittlung des Fingerabdrucks eines Gerätes erforderlichen Informationen zu sammeln.

Die Datenschutzrisiken beschränken sich nicht auf die Nachverfolgung (Tracking) durch Dritte. Die über Programmierschnittstellen (API) in der Software auf Client-Geräten erhältliche Kombination von Daten birgt ebenfalls das Risiko der Nutzung des virtuellen Fingerabdrucks. Verschiedene Software, Plattformen und API bieten jeweils Zugriff auf mehrere im Gerät gespeicherte Informationselemente. So kann beispielsweise die API für den Webbrowser und JavaScript Informationen über die Bildschirmgröße, die Farbtiefe und die verfügbaren Schriftarten liefern. Andere API können Zugang zu Informationselementen fordern, die in der Firmware (z. B. der Prozessortyp) oder auf der Grafikkarte gespeichert sind, oder erfragen, welches Betriebssystem verwendet wird.[22] API-Abfragen können auch das Vorhandensein von installierter Software (z. B. Browser-Plug-ins) oder sogar die genauen Versionsnummern offenlegen. Der Zugang zu solchen Datensätzen erhöht die Informationsdichte (Entropie) und somit das Risiko, dass Einzelpersonen über ihr Gerät identifiziert werden können.[23]

Im Gegensatz zu HTTP-Cookies können virtuelle Fingerabdrücke verdeckt genutzt werden.[24] Dem Nutzer stehen keine einfachen Mittel zur Verfügung, um dies zu verhindern, und es ist nur in eingeschränktem Maß möglich, Informationselemente, die zur Erzeugung des Fingerabdrucks verwendet werden, zurückzusetzen oder zu ändern. Folglich können virtuelle Fingerabdrücke von Dritten dazu genutzt werden, Nutzer verdeckt zu identifizieren oder herauszugreifen, um ihnen gezielt Inhalte zukommen zu lassen oder sie auf sonstige Weise unterschiedlich zu behandeln.

Gemäß der Stellungnahme 16/2011[25] haben Werbeunternehmen geltend gemacht, dass die Verwendung eindeutiger Codes oder sonstiger Werte nicht mit der Verarbeitung personenbezogener

---

[21] Eckersley, 2010. A Primer on Information Theory and Privacy.https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy

[22] Mowery, 2012. Pixel Perfect: Fingerprinting Canvas in HTML5. http://cseweb.ucsd.edu/~hovav/dist/canvas.pdf

[23] Mozilla, 2014. https://wiki.mozilla.org/Fingerprinting

[24] Nur in bestimmten Fällen wie der HTML5-Geolokalisierungs-API fordert das Protokoll ein Signal an den Nutzer. Siehe: http://www.w3.org/TR/geolocation-API/#privacy_for_uas.

[25] Artikel-29-Datenschutzgruppe, 2014. Stellungnahme 16/2011 zur Best-Practice-Empfehlung von EASA und IAB zu verhaltensorientierter Online-Werbung. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_de.pdf

Daten verbunden ist. Dies steht im Widerspruch zum Zweck der Verarbeitung für die Bereitstellung personalisierter Inhalte und Werbung, d. h. zur direkten Kommunikation mit einer bestimmten Person. Die Datenschutzgruppe hat wiederholt argumentiert, dass solche eindeutigen Merkmale als personenbezogene Daten einzustufen sind.[26]

6. Rechtsrahmen

Wird ein Fingerabdruck durch die Speicherung von Informationen generiert, die im Endgerät des Nutzers gespeichert sind, oder durch den Zugriff darauf, so gilt die e-Datenschutz-Richtlinie.

Wie in der Stellungnahme 04/2012 dargelegt, kann gemäß Artikel 5 Absatz 3 von dem Erfordernis der Einwilligung abgesehen werden, wenn eines der folgenden Kriterien erfüllt ist:

KRITERIUM A: technische Speicherung oder Zugang, „*wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist*".

KRITERIUM B: technische Speicherung oder Zugang, „*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*".

Darüber hinaus muss der Betreiber der Webpräsenz eindeutige andere Signale - so etwa den „Do-Not-Track"[27]-Header[28] - respektieren, die den entsprechenden Wunsch des Nutzers zum Ausdruck bringen.

Zwar ist die Anwendung der Datenschutzrichtlinie nicht Gegenstand dieser Stellungnahme, doch muss die Nutzung des virtuellen Fingerabdrucks, sofern sie eine Verarbeitung personenbezogener Daten darstellt, in Übereinstimmung mit den einschlägigen Bestimmungen dieser Richtlinie erfolgen.

Im Sinne von Artikel 5 Absatz 3 der e-Datenschutz-Richtlinie gilt das Erfordernis der Einwilligung des Nutzers für jede Partei, die beabsichtigt, im Endgerät des Nutzers gespeicherte Informationen zu speichern oder darauf zuzugreifen, selbst wenn diese Informationen noch nicht als personenbezogene Daten angesehen werden. Das Thema der Einwilligung wurde von der Artikel-29-Datenschutzgruppe in etlichen Stellungnahmen erörtert, sowohl allgemein[29] als auch im Hinblick auf verhaltensorientierte

[26] Artikel-29-Datenschutzgruppe, 2014. Stellungnahme 05/2014 zu Anonymisierungstechniken, S. 13 ff. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf

[27] W3C, Tracking Preference Expression (DNT). http://www.w3.org/TR/tracking-dnt/

[28] Das Do-Not-Track-Protokoll hat das Potenzial, sich unter bestimmten Umständen zu einem griffigen Einwilligungsmechanismus zu entwickeln, der im Einklang mit Erwägungsgrund 66 der Richtlinie 2009/136/EG steht. Dieser Erwägungsgrund sieht für Nutzer die Möglichkeit vor, ihre Einwilligung über ihre Browsereinstellungen zu erteilen, aber nur, wenn die Einwilligung den oben genannten Anforderungen an eine gültige Einwilligung entspricht. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140606_wp29_ts_standardisation_letter_to_w3c.pdf

[29] Artikel-29-Datenschutzgruppe, 2011. Stellungnahme 15/2011 zur Begriffsbestimmung der Einwilligung (in englischer Sprache). http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

Online-Werbung[30]. Die Datenschutzgruppe hat das Erfordernis der Einwilligung zudem im Kontext von Artikel 5 Absatz 3 und Cookies erörtert.[31]

Es sei an die Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten[32] erinnert, in der es heißt:

„Es ist wichtig, zwischen der für das Speichern und Lesen von Informationen auf dem Gerät erforderlichen Einwilligung und der Einwilligung zu unterscheiden, die als Rechtsgrundlage für die Verarbeitung verschiedener Arten personenbezogener Daten erforderlich ist. Beide Anforderungen gelten gleichzeitig […]. Daher können beide Einwilligungen in der Praxis gemeinsam eingeholt werden […]; Voraussetzung ist allerdings, dass der Nutzer unmissverständlich darüber informiert wird, wofür er seine Einwilligung erteilt."

Erwägungsgrund 66 der e-Datenschutz-Richtlinie spricht vom „*unberechtigten Eindringen in die Privatsphäre*" und Artikel 5 behandelt das Erfordernis der Vertraulichkeit der Kommunikation. Mit Artikel 5 Absatz 3 wird das Vertraulichkeitskriterium auf Informationen ausgedehnt, die auf dem Gerät des Nutzers gespeichert oder abgerufen werden. Daher fällt jegliche Verarbeitung seitens des Dritten, die das Verhalten des betreffenden Geräts beeinflusst oder es veranlasst, Informationen zu speichern oder Zugriff auf Informationen zu geben, die sich auf diesem Gerät befinden oder durch dieses abgerufen werden, in den Anwendungsbereich von Artikel 5 Absatz 3.

Die Verwendung der Begriffe „*gespeichert oder abgerufen*" deutet darauf hin, dass die Speicherung und der Zugriff nicht im Rahmen derselben Kommunikation erfolgen und nicht von derselben Partei vorgenommen werden müssen. Informationen, die von einer Partei gespeichert wurden (darunter vom Nutzer oder Hersteller des Geräts gespeicherte Informationen) und später von einer anderen Partei abgerufen werden, fallen daher in den Anwendungsbereich von Artikel 5 Absatz 3. Ein Beispiel wäre die App eines Mobiltelefons, mit der die Kontaktliste des Nutzers verarbeitet wird, wenn die Kontaktdetails vom Nutzer gespeichert, jedoch von einem Dritten abgerufen werden. Dies darf nicht dahingehend ausgelegt werden, dass der Dritte die Einwilligung zum Zugriff auf diese Informationen nicht braucht, nur weil er sie nicht gespeichert hat. Das Einwilligungserfordernis besteht auch für einen Lesezugriff auf einen Festwert (beispielsweise für die Abfrage der MAC-Adresse einer Netzschnittstelle über die OS-API).

Daher müssen Dritte bedenken, dass die Einwilligung (vorbehaltlich einer geltenden Ausnahmeregelung) erforderlich ist, wenn im Rahmen der Nutzung des virtuellen Fingerabdrucks auf dem Gerät des Nutzers befindliche Daten(sätze) gespeichert oder abgerufen werden sollen. Dies gilt auch für den Fall, dass einige dieser Informationselemente nicht die Speicherung von oder den Zugriff auf Informationen erfordern.

---

[30] Artikel-29-Datenschutzgruppe, 2010. Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_de.pdf

[31] Artikel-29-Datenschutzgruppe, 2013. Arbeitsunterlage 02/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_de.pdf

[32] Artikel-29-Datenschutzgruppe, 2013. Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_de.pdf

7. Verwendungsszenarien

7.1. Verwendung: First-Party-Webanalysen

Eine Reihe von Online-Diensten hat vorgeschlagen, als Alternative zu den HTTP-Cookies den virtuellen Fingerabdruck für die Zwecke der Analyse zu nutzen. Dies würde es ermöglichen, die in Artikel 5 Absatz 3 vorgesehene Einwilligung zu umgehen. In ihrer Stellungnahme 04/2012 hat die Datenschutzgruppe eingeräumt, dass ein drittes Kriterium für die Ausnahme von der Einwilligungspflicht für First-Party-Analysen eingeführt werden könnte,

„*wenn sie ausschließlich für die aggregierten Statistiken des Erstanbieters genutzt und von Websites verwendet werden, die in ihrer Datenschutzrichtlinie bereits unmissverständlich über diese Cookies informieren und ausreichende Datenschutzgarantien bieten. Diese Garantien sollten unter anderem eine benutzerfreundliche Möglichkeit zur Abwahl jedweder Datenerfassung sowie umfassende Anonymisierungsmechanismen für sonstige gesammelte Informationen wie etwa IP-Adressen, anhand derer Personen identifiziert werden können, beinhalten.*“

In der Stellungnahme wird jedoch auch darauf hingewiesen, dass derzeit für Cookies, die allein der Erstellung anonymisierter und aggregierter Statistiken des Erstanbieters dienen, derzeit keine Ausnahme von der Einwilligungspflicht besteht.[33] Daher fallen First-Party-Webanalysen mittels virtuellem Fingerabdruck nicht unter die Ausnahmeregelung nach Kriterium A oder B, so dass die Einwilligung des Nutzers erforderlich ist.

7.2. Verwendung: Nachverfolgung (Tracking) für verhaltensorientierte Online-Werbung

Viele Internetseiten enthalten Third-Party-Webbugs, Pixeltags und JavaScript-Code, um Werbedienstleistungen zu ermöglichen. Dies führt zu einer Reihe von Abfragen von Informationselementen vom Gerät des Nutzers. Diese Abfragen werden an Werbetreibende übermittelt und ermöglichen es ihnen, einen virtuellen Fingerabdruck zu erstellen, mit dem sie im Zeitlauf Nutzer über Websites hinweg verfolgen und ein Interessenprofil für gezielte Werbung erzeugen können, selbst wenn der Nutzer Cookies ablehnt. Dies kann technisch auf verdeckte Weise erfolgen, ohne dass der Nutzer etwas davon mitbekommt.

In der Stellungnahme 04/2012 wurde betont, dass Third-Party-Cookies zu Werbezwecken nicht unter die Ausnahmeregelung nach Kriterium A oder B fallen. Deshalb erfordert die Nutzung des virtuellen Fingerabdrucks zum Zwecke der gezielten Werbung die Einwilligung des Nutzers.

7.3. Verwendung: Netzwerkzugang

Die ordnungsgemäße Verwaltung eines Netzwerks erfordert die Übertragung bestimmter Informationselemente, die zu jedem an das Netzwerk angeschlossenen Gerät gehören. So verarbeitet ein WLAN-Zugangspunkt, der die Verbindung zwischen Drahtlosgeräten und einem verkabelten

[33] Artikel-29-Datenschutzgruppe, 2012. Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, S. 12.

Netzwerk verwaltet, eindeutige und nicht eindeutige Merkmale wie die MAC-Adresse[34] und den Kanal, um Verbindungen ordnungsgemäß aufrechtzuerhalten und Datenpakete korrekt weiterzuleiten.

Erfordert die Bereitstellung des Netzwerks Informationselemente, durch die Informationen auf dem Gerät des Nutzers gespeichert werden oder durch die auf diese zugegriffen wird, fällt dies in den Anwendungsbereich von Artikel 5 Absatz 3. Ist diese Datenverarbeitung für den normalen Betrieb des Netzwerks erforderlich, fällt dies unter die Ausnahmeregelung nach Kriterium A.

Die sekundäre Verwendung eines Informationselements oder eines virtuellen Fingerabdrucks für Tracking-Zwecke erfüllt nicht das Kriterium, dem zufolge „*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*". Im Zusammenhang mit Mehrzweck-Cookies stellte die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme 04/2012 fest, „*dass es höchst unwahrscheinlich [ist], dass das Tracking eines der Kriterien A oder B erfüllt*". Beabsichtigt ein Dritter also, einen virtuellen Fingerabdruck für verschiedene Zwecke zu verwenden, kann dies „*nur dann von der Einwilligungspflicht ausgenommen werden, wenn jeder einzelne Zweck [...] von der Einwilligungspflicht ausgenommen ist*".

7.4. Verwendung: Nutzerzugang und -kontrolle

Ein Online-Dienst könnte mit der Nutzung des virtuellen Fingerabdrucks das Ziel verfolgen, Nutzerzugang und -kontrolle zu unterstützen (d. h. in Verbindung mit einem Nutzernamen und Passwort). Der virtuelle Fingerabdruck kann genutzt werden, um zu gewährleisten, dass ein Konto an ein bestimmtes Gerät geknüpft ist, so dass das Gerät als zweiter Authentifizierungsfaktor fungiert.

Beispiel: Ein Musikabodienst gestattet einem Nutzer den Zugang nur von einer begrenzten Zahl bestimmter Geräte aus. Hat ein Nutzer zuvor ein bestimmtes Gerät verwendet, kann der Betreiber der Webpräsenz beschließen, weniger Überprüfungen vor der Gewährung des Zugangs durchzuführen.

Setzt sich ein virtueller Fingerabdruck aus Informationselementen zusammen, durch die Informationen auf dem Gerät des Nutzers gespeichert werden oder durch die auf diese zugegriffen wird, fällt dies in den Anwendungsbereich von Artikel 5 Absatz 3. Solche Zwecke sind jedoch nicht als „*unbedingt erforderlich*" für die Bereitstellung einer vom Nutzer ausdrücklich gewünschten Funktionalität anzusehen, so dass eine gültige Einwilligung des Nutzers erforderlich ist.

Website-Betreiber müssen ggf. eine Reihe geeigneter und verhältnismäßiger Kontrollen oder sonstiger Authentifizierungsverfahren (z. B. ein Einmal-Passwort, ergänzende Bestätigung per E-Mail) in Erwägung ziehen.

7.5. Verwendung: nutzerorientierte Sicherheit

In ihrer Stellungnahme 04/2012 hat die Artikel-29-Datenschutzgruppe dargelegt, dass *„Cookies [...], die ausschließlich der besseren Sicherheit des vom Nutzer ausdrücklich angeforderten Dienstes dienen"* (z. B. zur Entdeckung wiederholt fehlgeschlagener Anmeldeversuche) unter die Ausnahmeregelung nach Kriterium B fallen.

[34] Die MAC-Adresse dürfte bezüglich der an das Netzwerk angeschlossenen Geräte eindeutig sein. Das Präfix der MAC-Adresse verweist auch auf den Chiphersteller.

Diese Ausnahme würde auch für virtuelle Fingerabdrücke gelten, jedoch wie bei Cookies nicht für solche, *„die der Sicherheit von Websites oder Diensten Dritter dienen, die nicht ausdrücklich vom Nutzer angefordert wurden“*.

Soll die Erhebung von Daten über die Nutzung des virtuellen Fingerabdrucks einem nutzerorientierten Sicherheitszweck dienen, darf dieser Fingerabdruck nicht für sekundäre Zwecke verwendet werden, sonst ist seine Nutzung nicht von der Einwilligungspflicht ausgenommen. Es müssen technische und organisatorische Vorkehrungen getroffen werden, um eine sekundäre Nutzung von Fingerabdruckdaten zu verhindern, die in der Regel in Server-Sicherheitslogs enthalten sind.

7.6. Verwendung: Anpassung der Benutzeroberfläche an das Gerät

Zugang zu Geräteeinstellungen wie der Bildschirmgröße kann nützlich sein, um das Layout von Inhalten zu optimieren.[35] Beispielsweise könnte ein Medienportal in einen Modus mit weniger Grafikelementen oder einer nur einspaltigen Anzeige für Mobilgeräte wechseln. Auch könnten eine Website oder Dritte, die über diese Website Inhalte anbieten, das Gerät auf bestimmte technische Möglichkeiten überprüfen, z. B. daraufhin, welche Videoformate unterstützt werden.

Verfolgen Dritte mit dem Zugang zu Informationen, die auf dem Gerät des Nutzers gespeichert sind, ausschließlich den Zweck der Anpassung des Inhalts an die Merkmale des Geräts, so fällt dies unter KRITERIUM B. Somit ist für die kurzfristige Anpassung der Nutzeroberfläche keine Einwilligung erforderlich.

Werden diese Informationen jedoch auch für sekundäre Zwecke genutzt, gilt diese Ausnahmeregelung nicht mehr.

8. Schlussfolgerung

Diese Stellungnahme ist der Problematik des virtuellen Fingerabdrucks und der Frage gewidmet, ob Artikel 5 Absatz 3 der Richtlinie 2002/58/EG (e-Datenschutz-Richtlinie), geändert durch die Richtlinie 2009/136/EG, unbeschadet der Bestimmungen der Datenschutz-Richtlinie 95/46/EG auf den virtuellen Fingerabdruck anwendbar ist. Diese Stellungnahme geht über die frühere Stellungnahme 04/2012 (Ausnahme von Cookies von der Einwilligungspflicht) hinaus und bestätigt, dass diese Technologie in einer Reihe von Fällen dazu führt, dass Informationen vom Endgerät des Nutzers abgerufen oder dort gespeichert werden. Somit gilt Artikel 5 Absatz 3 der e-Datenschutz-Richtlinie auch für Fälle der Nutzung des virtuellen Fingerabdrucks.

Deshalb müssen Parteien, die virtuelle Fingerabdrücke verarbeiten wollen, die bei dem Zugriff auf oder der Speicherung von Informationen auf dem Endgerät des Nutzers generiert wurden, zuerst die gültige Einwilligung des Nutzers erhalten (sofern nicht eine Ausnahmeregelung gilt).

[35] Es sei darauf hingewiesen, dass es andere, weniger in die Privatsphäre eingreifende Methoden zur Erreichung des gleichen Ziels geben kann, beispielsweise die Verwendung der Zeichenfolge des Benutzeragenten.