GROEP GEGEVENSBESCHERMING ARTIKEL 29

14/NL
WP 224

Advies 9/2014 over de toepassing van Richtlijn 2002/58/EG op device fingerprinting

Goedgekeurd op 25 november 2014

De groep is opgericht op grond van artikel 29 van Richtlijn 95/46/EG. Het is een onafhankelijk Europees adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer, waarvan de taken zijn omschreven in artikel 30 van Richtlijn 95/46/EG en in artikel 15 van Richtlijn 2002/58/EG.

Het secretariaat wordt verzorgd door Directoraat C (grondrechten en burgerschap van de Unie) van het directoraat-generaal Justitie van de Europese Commissie, 1049 Brussel, België, kamer MO-59 02/013.

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

DE GROEP VOOR DE BESCHERMING VAN PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSGEGEVENS

Ingesteld bij Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995,

Gezien artikel 29 en 30 van die richtlijn,

Gezien het reglement van orde van de Groep,

HEEFT HET VOLGENDE ADVIES VASTGESTELD:

1. SAMENVATTING

Het nemen van digitale vingerafdrukken van apparatuur (ook wel "device fingerprinting" genoemd) vormt een ernstig probleem voor de gegevensbescherming van particulieren. Zo heeft een aantal onlinediensten bijvoorbeeld voorgesteld om device fingerprinting als alternatief voor HTTP-cookies in te zetten voor doeleinden als het verschaffen van analyses of het traceren zonder toestemmingsverplichting op grond van artikel 5, lid 3[1]. Dit laat zien dat de met device fingerprinting samenhangende risico's niet slechts theoretisch van aard zijn. Bovendien blijkt uit onderzoek dat device fingerprinting reeds wordt toegepast[2].

In dit advies richt de Groep gegevensbescherming artikel 29 (WP29) zich op het onderwerp van device fingerprinting en de toepasselijkheid van artikel 5, lid 3, van de e-privacyrichtlijn 2002/58/EG, zoals gewijzigd bij Richtlijn 2009/136/EG, onverminderd de bepalingen van de richtlijn gegevensbescherming 95/46/EG. De belangrijkste boodschap van dit advies is dat artikel 5, lid 3, van de e-privacyrichtlijn van toepassing is op device fingerprinting.

Dit advies vormt een uitbreiding op het eerdere advies 04/2012 over ontheffing van de toestemmingsverplichting voor cookies[3] en bepaalt dat het derden[4] die digitale vingerafdrukken van apparatuur verwerken die worden gegenereerd door het verkrijgen van toegang tot of het opslaan van informatie op de eindapparatuur van de gebruiker, daarvoor de geldige toestemming van de gebruiker moeten hebben (tenzij een ontheffing van kracht is).

2. Inleiding

Artikel 5, lid 3, van Richtlijn 2002/58/EG, zoals gewijzigd bij Richtlijn 2009/136/EG,[5] (de e-privacyrichtlijn) bepaalt dat lidstaten ervoor moeten zorgen dat *"de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker"* alleen is toegestaan wanneer de betrokken abonnee of gebruiker toestemming heeft verleend op basis van duidelijke en volledige informatie die hem overeenkomstig Richtlijn 2002/58/EG[6] (de richtlijn gegevensbescherming) is verstrekt, onder meer over de doeleinden van de verwerking[7].

---

[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] Groep gegevensbescherming artikel 29, 2012. Advies 04/2012 over ontheffing van de toestemmingsverplichting voor cookies. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_nl.pdf

[4] "Derden" zoals bedoeld in overweging 66 van Richtlijn 2009/136/EG

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

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

[7] Zulks vormt geen beletsel voor enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk, of, indien

In haar advies 04/2012 heeft de Groep artikel 29 artikel 5, lid 3, van de e-privacyrichtlijn onderzocht met betrekking tot de opslag van of toegang tot informatie door middel van het gebruik van cookies. Het advies stelde dat artikel 5, lid 3, niet uitsluitend van toepassing is op cookies, maar ook op "soortgelijke technologieën".

In dit advies wordt ingegaan op het toenemend aantal meldingen dat derde partijen voor talrijke doeleinden actief op zoek zijn naar alternatieve technologieën voor cookies in een poging de toestemmingsverplichting van artikel 5, lid 3, te omzeilen. Met name de combinatie van een aantal informatie-elementen voor de unieke identificatie van specifieke apparatuur of applicaties, het zogenaamde "device fingerprinting", wordt onderzocht.

Digitale vingerafdrukken van apparatuur kunnen ook persoonlijke gegevens vormen. Dit advies voorziet niet in een analyse van de relevante bepalingen van de richtlijn gegevensbescherming, maar verwijst naar vraagstukken inzake gegevensbescherming die met name relevant zijn in het kader van device fingerprinting, bijvoorbeeld wanneer een aantal informatie-elementen, met name unieke identificatoren zoals IP-adressen, wordt gecombineerd en het doel van deze verwerking erin bestaat gebruikers in de tijd en voor verschillende websites te identificeren, zoals gebeurt voor reclame op basis van surfgedrag. In dergelijke gevallen moet de verwerking ook voldoen aan de in de richtlijn gegevensbescherming vastgelegde voorschriften.

De technologie van device fingerprinting beperkt zich niet tot de configuratieparameters van een traditionele webbrowser op een desktopcomputer. Device fingerprinting is bovendien niet gebonden aan een bepaald protocol, maar kan worden gebruikt om vingerafdrukken te nemen van een groot aantal op het internet aangesloten apparaten, consumentenelektronica en -toepassingen, waaronder de applicaties die draaien op mobiele apparaten, smart-tv's, spelcomputers, e-bookreaders, internetradio's, in auto's geïntegreerde systemen of slimme meters[8].

3. Definitie

RFC6973[9] definieert een vingerafdruk als een verzameling van informatie-elementen waarmee een apparaat of applicatie kan worden geïdentificeerd. De term wordt in dit advies in ruime zin toegepast en omvat tevens informatie die kan worden gebruikt om gebruikers, useragents of het apparaat in de tijd te herleiden[10], te koppelen[11] of te deduceren[12]. Dit betreft onder meer gegevens die zijn verkregen door middel van:

---

strikt noodzakelijk, voor de levering van een uitdrukkelijk door de abonneegebruiker gevraagde dienst van de informatiemaatschappij.

[8] Ook wel "het internet van dingen" genoemd.

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

[10] *Herleidbaarheid*: de mogelijkheid om een persoon in de dataset te individualiseren door sommige of alle records uit te lichten, advies 05/2014 over anonimiseringstechnieken, blz. 11-12.

[11] *Koppelbaarheid*: de mogelijkheid om ten minste twee records over dezelfde betrokkene of groep betrokkenen met elkaar in verband te brengen (in dezelfde database of in twee verschillende databases). Wanneer een aanvaller (bijvoorbeeld door de correlatie te analyseren) kan vaststellen dat twee records aan een en dezelfde groep personen zijn gerelateerd, zonder personen binnen deze groep te kunnen identificeren,

(a) de configuratie van een useragent/apparaat; of

(b) gegevens die worden vrijgegeven door het gebruik van netwerkcommunicatieprotocollen.

Een vingerafdruk kan zijn opgebouwd uit veel verschillende soorten data, waaronder:

(a) CSS-informatie;

(b) JavaScript-objecten (bijv. document, venster, scherm, navigator, datum en taal);

(c) HTTP-headerinformatie (bijv. het aantal bits aan informatie in de useragentstring, de indeling van de HTTP-header, verschillen in HTTP-header per requesttype);

(d) klokinformatie (bijv. clock skew (niet-synchronisatie kloksignaal) en klokfout);

(e) verschillen in TCP-stack;

(f) geïnstalleerde lettertypen;

(g) geïnstalleerde plugin-informatie (bijv. configuratie en versie-informatie)[13];

(h) het gebruik van interne applicatieprogramma-interfaces[14] (API's) die zijn vrijgegeven door de useragent/het apparaat; of

(i) het gebruik van externe API's van webdiensten waarmee de useragent/het apparaat communiceert.

4. Technische achtergrond

Het internet en het web zijn ontwikkeld met in gedachten de behoeften aan een veerkrachtige en open architectuur van de netwerkomgeving[15]. Om in deze behoeften te voorzien, zijn er ontwerpkeuzes gemaakt waardoor apparaten informatie-elementen uitzenden. Een aantal protocollen omvat een reeks verplichte en optionele informatie-elementen. Het HTTP/1.1-[16]protocol specificeert bijvoorbeeld headervelden waardoor de server en de client aanvullende informatie met betrekking tot de hypertekst kunnen opnemen. Sommige van deze protocollen zijn specifiek bedoeld voor de server om clienttypen

---

dan doorstaat de techniek de "herleidbaarheidstoets", maar niet de koppelbaarheidstoets, advies 05/2014 over anonimiseringstechnieken, blz. 11-12.

[12] *Deduceerbaarheid*: de mogelijkheid om de waarde van een persoonskenmerk ("attribuut") met grote waarschijnlijkheid af te leiden uit de waarden van een reeks andere attributen, advies 05/2014 over anonimiseringstechnieken, blz. 11-12.

[13] *Cf.* (a) http://www.w3.org/wiki/Fingerprinting, (b) http://w3c.github.io/fingerprinting-guidance/#wsj-orbitz (c) https://wiki.mozilla.org/Fingerprinting en (d) https://trac.webkit.org/wiki/Fingerprinting for mechanisms.

[14] De API biedt een gebruiksvriendelijk kader voor de toegang tot functies of routines binnen een softwarecomponent.

[15] Kahn, 1972. Communications principles for operating systems. Intern BBN-memorandum.

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

te herkennen. Zo bevat het headerveld van het request van de useragent de beschrijving: *"Dit is voor statistische doeleinden, het traceren van protocolovertredingen en het automatisch herkennen van useragents omwille van responsen op maat en het voorkomen van specifieke useragent-beperkingen."*

Useragentstrings worden doorgaans onder meer gebruikt om de opmaak van de inhoud van een bepaald soort apparaat te optimaliseren, om deze informatie aan specifieke gebruikers te richten[17]; of om informatie over het apparaat te verzamelen voor beveiligings- of statistische doeleinden.

5. Risico's voor de bescherming van gegevens

Aangezien een afzonderlijke HTTP-header doorgaans niet over een unieke waarde beschikt, kunnen gebruikers maar zelden individueel worden geïdentificeerd op grond van het informatie-element alleen[18]. De verschillende soorten media die door een browser worden ondersteund, worden vaak door veel dezelfde gebruikers met dezelfde browserversie gebruikt. Wanneer deze niet-unieke informatie-elementen dus afzonderlijk worden verwerkt, leveren ze doorgaans geen risico's voor de bescherming van gegevens op.

Een aantal informatie-elementen kan echter worden samengevoegd tot een verzameling die voldoende uniek is (vooral wanneer deze wordt gecombineerd met andere identificatoren, zoals het oorspronkelijke IP-adres) om als unieke vingerafdruk voor het apparaat of de applicatie te fungeren. Met behulp van deze vingerafdruk kan het ene apparaat van het andere worden onderscheiden en de vingerafdruk kan als verborgen alternatief voor cookies worden gebruikt om het internetgedrag in de tijd te volgen[19, 20, 21]. Op deze manier kan een individu aan de hand van de vingerafdruk van dat apparaat in verband worden gebracht, en dus worden geïdentificeerd, of identificeerbaar worden gemaakt.

De risico's inzake gegevensbescherming bij device fingerprinting zijn hoger doordat de unieke verzameling van informatie-elementen niet alleen voor de uitgever van de website toegankelijk is, maar ook voor vele andere derde partijen. Deze risico's staan haaks op het beleid inzake dezelfde oorsprong bij HTTP-cookies en worden nog eens versterkt door het technisch karakter van het internet, aangezien veel derde partijen bijdragen tot de inhoud van een webpagina.

Het is gebruikelijk dat een afzonderlijke webpagina op niet-statische wijze in realtime wordt gegenereerd door de inhoud ervan uit diverse bronnen op te vragen. Elk van deze bronnen zal afzonderlijk de HTTP-requests genereren, en afbeeldingen, JavaScript en CSS-bestanden downloaden. Veel webpagina's bevatten eveneens webtaps en trackingscripts. Ook kunnen deze webpagina's

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

[18] Er zijn gevallen waarin een afzonderlijk informatie-element informatie draagt waarmee een betrokkene eenduidig kan worden geïdentificeerd, zoals een OAuth-toegangstoken.

[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

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

http-requests indienen die registreren wanneer een gebruiker over een pagina, afbeelding of advertentie scrolt of erop klikt. Derden hebben derhalve regelmatig de kans om de informatie te verzamelen die nodig is voor het nemen van de vingerafdrukken van het apparaat van de gebruiker.

Risico's met betrekking tot de bescherming van gegevens blijven niet beperkt tot het traceren van gebruikers door derden. De combinatie van gegevens die aan de hand van de in de software op clientapparatuur aanwezige applicatieprogramma-interfaces (API) wordt verkregen, is tevens een risico van device fingerprinting. De verschillende software, platformen en API's bieden elk toegang tot verschillende in het apparaat opgeslagen informatie-elementen. Zo kan de JavaScript-API van de webbrowser bijvoorbeeld informatie verschaffen over de schermgrootte, de kleurdiepte en de beschikbare systeemlettertypen. Andere API's kunnen toegang vragen tot informatie-elementen die opgeslagen liggen in de firmware (bijv. het type CPU), het besturingssysteem (bijv. het type OS) of het model grafische kaart[22]. Door middel van het aanroepen van API's kan ook de aanwezigheid van geïnstalleerde software zichtbaar worden (bijv. plug-ins) of zelfs de exacte versienummers. Door de toegang tot deze informatie neemt het aantal bits aan informatie (entropie of informatiedichtheid) toe en daarmee ook het risico op herkenning van afzonderlijke individuen aan de hand van hun apparatuur[23].

In tegenstelling tot HTTP-cookies kan device fingerprinting heimelijk plaatsvinden[24]. Er bestaan geen eenvoudige middelen voor gebruikers om deze activiteit te voorkomen en er is slechts een beperkt aantal mogelijkheden voorhanden om de informatie-elementen die worden gebruikt voor het nemen van de digitale vingerafdruk, te resetten of te wijzigen. Op deze manier kunnen digitale vingerafdrukken van apparaten door derden worden gebruikt om gebruikers stiekem te identificeren of te herleiden en zo de mogelijkheid te creëren om ze inhoud toe te sturen of ze anderszins op specifieke wijze te benaderen.

In advies 16/2011[25] wordt geconstateerd dat reclamebureaus beweren dat bij het gebruik van unieke codes of andere waarden geen persoonlijke gegevens worden verwerkt. Dit is in tegenspraak met het doel van de verwerking, namelijk het leveren van gepersonaliseerde inhoud en reclame, dat wil zeggen het rechtstreeks communiceren met een specifiek persoon. De Groep heeft er herhaaldelijk op gewezen dat dergelijke unieke identificatoren als persoonsgegevens kunnen worden aangemerkt[26].

---

[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] Alleen in specifieke gevallen vereist het protocol dat er een melding aan de gebruiker wordt verzonden, zoals bij de geolocatie-API-specificatie van HTML5. Zie: http://www.w3.org/TR/geolocation-API/#privacy_for_uas.

[25] Groep gegevensbescherming artikel 29, 2014. Advies 16/2011 over de Best Practice Recommendation on Online Behavioural Advertising van EASA/IAB. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_nl.pdf

[26] Groep gegevensbescherming artikel 29, 2014. Advies 05/2014 over anonimiseringstechnieken, nlz. 11-12. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_nl.pdf

6. Rechtskader

Wanneer een vingerafdruk is genomen door de opslag van of de toegang tot informatie op de eindapparatuur van de gebruiker, is de e-privacyrichtlijn van toepassing.

Zoals beschreven in advies 04/2012 voorziet artikel 5, lid 3, erin dat de verwerking is ontheven van de toestemmingsverplichting, mits aan een van de volgende criteria is voldaan:

CRITERIUM A: technische opslag of toegang met *"als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk"*.

CRITERIUM B: technische opslag of toegang wanneer het "*strikt noodzakelijk is dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij deze dienst levert*".

Bovendien moet de website-exploitant de vastgelegde betekenis van elke andere voorkeursaanduiding van de gebruiker in dit verband respecteren, zoals de Do Not Track-header[27, 28].

Hoewel de toepassing van de richtlijn gegevensbescherming buiten het bestek van dit advies valt, dient te worden opgemerkt dat aangezien er bij device fingerprinting sprake is van de verwerking van persoonsgegevens, het belangrijk is dat device fingerprinting plaatsvindt in overeenstemming met elke relevante bepaling van deze richtlijn.

In artikel 5, lid 3, van de e-privacyrichtlijn wordt de toestemmingsverplichting vastgesteld van de gebruiker voor elke partij die van plan is om informatie op het eindapparaat van de gebruiker op te slaan of hier toegang toe te verkrijgen, zelfs als die informatie nog niet wordt aangemerkt als persoonlijke informatie. De Groep heeft de toestemming reeds in een aantal adviezen behandeld, zowel in algemene zin[29] als in specifiek opzicht in verband met reclame op basis van surfgedrag[30]. De Groep heeft de toestemmingsverplichting in het kader van artikel 5, lid 3, en cookies al behandeld[31].

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

[28] Het Do Not Track-protocol heeft de potentie om onder bepaalde omstandigheden uit te groeien tot een granulair toestemmingsmechanisme dat in overeenstemming is met overweging 66 van Richtlijn 2009/136/EG. Deze overweging stelt gebruikers in staat om hun toestemming middels hun browserinstellingen kenbaar te maken, op voorwaarde dat de toestemming voldoet aan de hierboven genoemde vereisten voor geldige toestemming. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140606_wp29_ts_standardisation_letter_to_w3c.pdf

[29] Groep gegevensbescherming artikel 29, 2011. Advies 15/2011 over de definitie van toestemming. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

[30] Groep gegevensbescherming artikel 29, 2010. Advies 2/2010 over online reclame op basis van surfgedrag ("behavioural advertising"). http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

[31] Groep gegevensbescherming artikel 29, 2013. Werkdocument 02/2013 met richtsnoeren voor het verkrijgen van toestemming voor cookies. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

Hierbij kan advies 02/2013 betreffende apps op intelligente apparaten[32] worden aangehaald, waarin staat:

"het onderscheid tussen de toestemming die vereist is om informatie op het apparaat te plaatsen en te lezen, en toestemming als wettelijke grond voor de verwerking van verschillende soorten persoonsgegevens. Hoewel beide vormen van toestemming tegelijkertijd van toepassing zijn, [...] kunnen beide soorten toestemming derhalve in de praktijk worden samengevoegd, op voorwaarde dat de gebruiker er op ondubbelzinnige wijze op wordt gewezen waarmee hij instemt."

Overweging 66 van de e-privacyrichtlijn verwijst naar *"ongeoorloofde indringing in de privésfeer"* en artikel 5 heeft betrekking op de vertrouwelijkheidsvereiste van het communicatieverkeer. Artikel 5, lid 3, kan worden beschouwd als een uitbreiding van de vertrouwelijkheid van informatie naar informatie die wordt opgeslagen of opgeroepen op het apparaat van de gebruiker. Daarom valt elke verwerking door een derde partij die van invloed is op het gedrag van dat apparaat of waarbij de derde partij anderszins informatie op dat apparaat opslaat of raadpleegt, of die wordt vrijgegeven door dat apparaat, binnen de werkingssfeer van artikel 5, lid 3.

De termen *"opgeslagen of geraadpleegd"* geven aan dat de opslag en toegang niet noodzakelijkerwijs binnen dezelfde communicatiestroom moeten plaatsvinden of door dezelfde partij moeten worden uitgevoerd. Informatie die is opgeslagen door een partij (waaronder informatie die is opgeslagen door de gebruiker of de fabrikant van het apparaat), en die vervolgens wordt geraadpleegd door een andere partij, valt dan ook binnen de werkingssfeer van artikel 5, lid 3. Een voorbeeld hiervan is een mobiele-telefoonapp die de lijst met contactpersonen van de gebruiker verwerkt op grond van de door de gebruiker zelf opgeslagen contactgegevens, terwijl de toegang tot deze lijst wordt verzorgd door de derde partij. Het is niet juist om basis hiervan af te leiden dat de derde partij geen toestemming nodig heeft om zich toegang te verschaffen tot deze informatie, omdat zij niet verantwoordelijk was voor de opslag ervan. De toestemmingsverplichting geldt ook wanneer toegang wordt verschaft tot een "Alleen lezen"-waarde (bijv. het verzoek tot het MAC-adres van een netwerkinterface via de OS-API).

Het is dus belangrijk voor een derde partij om te onthouden dat, wanneer in het kader van device fingerprinting de opslag van, of de toegang tot (een verzameling van) informatie op het apparaat van de gebruiker nodig is, er toestemming vereist zal zijn (tenzij er een geldige vrijstelling van toepassing is). Dit geldt zelfs al is voor sommige van die informatie-elementen de opslag van, of toegang tot informatie niet noodzakelijk.

7. Scenario's van gebruiksgevallen

7.1. Gebruiksgeval: websiteanalyse door de eigen partij

Een aantal onlinediensten heeft voorgesteld om device fingerprinting als alternatief voor http-cookies in te zetten voor het leveren van analyses zonder dat toestemming op grond van artikel 5, lid 3 vereist wordt. In advies 04/2012 heeft de Groep de noodzaak erkend van een derde ontheffing voor de toestemmingsverplichting voor de analyse door de eigen partij:

"indien zij strikt worden beperkt tot geaggregeerde statistieken ten behoeve van de website-exploitant en worden ingezet door websites die in hun privacybeleid al duidelijke informatie geven over deze

[32] Groep gegevensbescherming artikel 29, 2013. Advies 02/2013 betreffende apps op intelligente apparaten. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_nl.pdf

cookies en passende privacywaarborgen bieden. In ieder geval mag de gebruiker verwachten dat hij op gebruiksvriendelijke wijze toestemming kan weigeren voor het verzamelen van zijn gegevens en dat de website-exploitant mechanismen toepast om andere reeds verzamelde identificerende informatie, zoals het IP-adres, volledig te anonimiseren."

In het advies werd echter ook gesteld dat er momenteel geen ontheffing geldt voor de toestemming voor cookies die strikt beperkt zijn tot cookies van de eerste partij ten behoeve van geanonimiseerde en geaggregeerde statistische doeleinden[33]. Websiteanalyse door de eigen partij door middel van device fingerprinting valt dus niet onder een ontheffing op grond van CRITERIUM A of B; derhalve is de toestemming van de gebruiker vereist.

7.2. Gebruiksgeval: tracking ten behoeve van reclame op basis van surfgedrag

Veel websites bevatten webtaps, pixeltags en JavaScript-code om reclamediensten mogelijk te maken. Dit leidt tot een aantal verzoeken om informatie-elementen op het apparaat van de gebruiker. Deze verzoeken worden doorgegeven aan de derde partijen die reclamediensten verzorgen, waardoor deze in staat worden gesteld om een vingerafdruk van het apparaat te nemen en zo gebruikers te volgen over websites en in de tijd, en een interesseprofiel voor gerichte reclame te creëren, zelfs al wijst deze gebruiker het gebruik van cookies af. Deze verwerking kan technisch gezien op een verborgen manier en dus zonder medeweten van de gebruiker worden uitgevoerd.

In advies 04/2012 wordt benadrukt dat reclame door derde partijen niet valt onder de ontheffing op grond van CRITERIUM A of B. Daarom is voor device fingerprinting met als doel gerichte reclame de toestemming van de gebruiker vereist.

7.3. Gebruiksgeval: netwerkdiensten

Voor een juist netwerkbeheer is de overdracht van bepaalde informatie-elementen met betrekking tot elk apparaat op het netwerk vereist. Zo zal bijvoorbeeld een wifi-toegangspunt, waar de verbinding tussen de draadloze apparaten en een bedraad netwerk wordt beheerd, unieke en niet-unieke informatie-elementen verwerken, zoals het MAC-adres[34] en het kanaal, om de verbindingen op de juiste wijze in stand te houden en de datapakketten op de juiste wijze te verzenden.

Indien voor de netwerkvoorziening informatie-elementen nodig zijn waarvoor de opslag van of de toegang tot informatie op het apparaat van de gebruiker noodzakelijk is, zal dit binnen de werkingssfeer van artikel 5, lid 3, vallen. Indien deze verwerking vereist is voor de normale werking van het netwerk, dan zou voor deze verwerking ontheffing op grond van criterium A gelden.

Het secundair gebruik van een informatie-element of vingerafdruk van een apparaat ten behoeve van tracking wordt niet beschouwd te hebben *"als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk"* of als *"strikt noodzakelijk om ervoor te zorgen dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de*

[33] Groep gegevensbescherming artikel 29, 2012. Advies 04/2012 over ontheffing van de toestemmingsverplichting voor cookies, blz. 10-11.

[34] Dit Mac-adres zal waarschijnlijk uniek zijn onder alle apparaten op het netwerk. Het voorvoegsel van het MAC-adres zal bovendien verwijzen naar de chipfabrikant.

informatiemaatschappij deze dienst levert". De Groep stelde in haar advies 04/2012 met betrekking tot de overwegingen aangaande de voor meerdere doeleinden bestemde cookies vast dat *"het zeer onwaarschijnlijk is dat het traceren van de gebruiker onder CRITERIUM A of B valt"* en dat, indien een derde partij een vingerafdruk van een apparaat voor meerdere doeleinden wenst te gebruiken, deze vingerafdruk alleen *"kan worden ontheven van de toestemmingsverplichting als alle onderscheiden doeleinden [...] niet toestemmingsplichtig zijn"*.

7.4. Gebruiksgeval: gebruikerstoegang en -controle

Een onlinedienst kan voornemens zijn de vingerafdrukken van het apparaat te gebruiken voor het ondersteunen van de gebruikerstoegang en het gebruikersbeheer (dat wil zeggen in combinatie met een gebruikersnaam en wachtwoord). De digitale vingerafdruk van het apparaat kan worden gebruikt om ervoor te zorgen dat een account is gekoppeld aan een specifiek apparaat, waardoor het apparaat fungeert als een tweede factor voor authenticatie.

Een muziekdienst op basis van een abonnement verleent de gebruiker slechts toegang tot de dienst vanaf een beperkt aantal specifieke apparaten. Wanneer een gebruiker een specifiek apparaat eerder heeft gebruikt, kan de website-exploitant ervoor kiezen om minder verificatiecontroles uit te voeren voor toegang.

Wanneer een digitale vingerafdruk van een apparaat is opgebouwd uit informatie-elementen waarvoor de opslag van of de toegang tot informatie op het apparaat van de gebruiker noodzakelijk is, zal dit binnen de werkingssfeer van artikel 5, lid 3, vallen. Dergelijke doeleinden zouden echter niet als *"strikt noodzakelijk"* worden beschouwd om een functionaliteit op uitdrukkelijk verzoek van de gebruiker te verlenen en daarom is de geldige toestemming van de gebruiker in dit geval vereist.

Mogelijk dienen website-exploitanten een reeks geschikte en evenredige controles of enige andere authenticatiemethode (bijv. een eenmalig wachtwoord, secundaire e-mailbevestiging) in overweging te nemen.

7.5. Gebruiksgeval: op de gebruiker gerichte beveiliging

In advies 04/2012 stelt de Groep dat *"cookies die specifiek worden ingezet om de beveiliging van de door de gebruiker uitdrukkelijk gevraagde dienst van de informatiemaatschappij te verbeteren"* (bijv. voor de detectie van herhaalde foutieve inlogpogingen) zouden worden ontheven op grond van CRITERIUM B.

Deze ontheffing zou ook gelden voor device fingerprinting, maar, net als voor cookies *"niet voor het gebruik van de techniek die verband houdt met de beveiliging van websites of diensten van derden waarom de gebruiker niet uitdrukkelijk heeft gevraagd"*.

Wanneer gegevens worden verzameld via device fingerprinting in het kader van een op de gebruiker gerichte beveiliging, mogen deze gegevens, om in aanmerking te komen voor de toestemmingsontheffing, niet worden gebruikt voor secundaire doeleinden. Er moeten technische en organisatorische veiligheidsmaatregelen worden genomen om elk secundair gebruik van de gegevens van digitale vingerafdrukken, die doorgaans worden bewaard in serverbeveiligingslogboeken, te voorkomen.

7.6. Gebruiksgeval: aanpassing van de gebruikersinterface op grond van het apparaat

Toegang tot informatie over het apparaat, zoals de schermgrootte, kan nuttig zijn om de lay-out van de inhoud te optimaliseren[35]. Zo kan een mediawebsite bijvoorbeeld overschakelen op een grafische modus van lage kwaliteit of een lay-out met een enkele kolom voor mobiele apparaten. Anderzijds is het mogelijk dat een website, of de derde partij die via die website inhoud verstrekt, het apparaat verzoekt om de technische mogelijkheden na te gaan, zoals welke videoformaten worden ondersteund.

Wanneer een derde partij toegang tot informatie vraagt die is opgeslagen op het apparaat van de gebruiker met als enig doel de inhoud ervan aan te passen aan de eigenschappen van het apparaat, dan geldt CRITERIUM B. Dit betekent dat voor de aanpassing van de gebruikersinterface op de korte termijn geen toestemming nodig is.

Indien deze informatie echter ook voor secundaire doeleinden wordt gebruikt, is deze ontheffing niet langer van kracht.

8. Conclusie

In dit advies wordt het onderwerp van device fingerprinting behandeld en de toepasselijkheid van artikel 5, lid 3, van de e-privacyrichtlijn 2002/58/EG, zoals gewijzigd bij Richtlijn 2009/136/EG, onverminderd de bepalingen van de richtlijn gegevensbescherming 95/46/EG. Dit advies vormt een uitbreiding op het eerdere advies 04/2012 over ontheffing van de toestemmingsverplichting voor cookies en bevestigt dat de technologie in een aantal gevallen leidt tot het verkrijgen van toegang tot of het opslaan van informatie op de eindapparatuur van de gebruiker. Artikel 5, lid 3, van de e-privacyrichtlijn is derhalve ook van toepassing wanneer sprake is van device fingerprinting.

Daarom mogen partijen de digitale vingerafdrukken van apparatuur die gegenereerd worden door het verkrijgen van toegang tot of het opslaan van informatie op de eindapparatuur van de gebruiker, uitsluitend verwerken met de geldige toestemming van de gebruiker (tenzij een ontheffing van kracht is).

[35] Er kunnen wel andere, meer privacyrespecterende methoden bestaan om hetzelfde doel te bereiken, waaronder het gebruik van de useragentstring.