ARTICLE 29 DATA PROTECTION WORKING PARTY

14/EN
WP 224

Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting

Adopted on 25 November 2014

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

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

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

Having regard to Articles 29 and 30 thereof,

Having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT OPINION:

1. Summary

Device fingerprinting presents serious data protection concerns for individuals. For example, a number of online services have proposed device fingerprinting as an alternative to HTTP cookies for the purpose of providing analytics or for tracking without the need for consent under Article 5(3).[1] This demonstrates that the risks presented by device fingerprinting are not theoretical and research has shown that device fingerprinting is already being exploited.[2]

In this Opinion, the Article 29 Working Party (WP29) addresses the topic of device fingerprinting and the applicability of Article 5(3) of the ePrivacy Directive 2002/58/EC, as amended by Directive 2009/136/EC, without prejudice to the provisions of the Data Protection Directive 95/46/EC. The key message of this Opinion is that Article 5(3) of the ePrivacy Directive is applicable to device fingerprinting.

This Opinion expands upon the earlier Opinion 04/2012 on Cookie Consent Exemption[3] and indicates to third-parties[4] who process device fingerprints which are generated through the gaining of access to or the storing of information on the user's terminal device that they may only do so with the valid consent of the user (unless an exemption applies).

2. Introduction

Article 5(3) of Directive 2002/58/EC as amended by Directive 2009/136/EC,[5] (the ePrivacy Directive) stipulates that Member States shall ensure that "*the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user"* is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information in accordance with Directive 95/46/EC[6] (the Data Protection Directive), inter alia, about the purposes of the processing.[7]

In Opinion 04/2012, WP29 considered Article 5(3) of the ePrivacy Directive in relation to the storage of, or access to, information through the use of cookies. The Opinion stated that Article 5(3) does not exclusively apply to cookies but is also applicable to "similar technologies".

[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] Article 29 Working Party, 2012. Opinion 04/2012 on Cookie Consent Exemption. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

[4] "Third-party" as referred to in Recital 66 of Directive 2009/136/EC

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

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

[7] This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

This Opinion addresses growing reports that third-parties are actively exploring alternative technologies to cookies for a range of purposes in an effort to avoid the consent requirement of Article 5(3). In particular, the combination of a set of information elements in order to uniquely identify particular devices or application instances, so-called "device fingerprinting", is examined.

Device fingerprints can also constitute personal data. This Opinion does not provide an analysis of the relevant provisions of the Data Protection Directive, but refers to data protection issues which are particularly relevant in the context of device fingerprinting. For example, when several information elements are combined, especially unique identifiers such as an IP addresses, and the purpose of the processing is to identify users over time, across websites, such as with behavioural advertising. In such cases, processing must also comply with the rules provided in the Data Protection Directive.

The technology of device fingerprinting is not limited to the configuration parameters of a traditional web browser on a desktop PC. Device fingerprinting is not tied to a particular protocol either, but can be used to fingerprint a broad range of internet connected devices, consumer electronics and applications, including those running on mobile devices, smart TVs, gaming consoles, e-book readers, internet radio, in-car systems or smart meters.[8]

3. Definition

RFC6973[9] defines a fingerprint as "a set of information elements that identifies a device or application instance". This Opinion uses the term in a broad sense, meaning that it includes a set of information that can be used to single out[10], link[11] or infer[12] a user, user agent or device over time. This includes, but is not limited to, data derived from:

(a) the configuration of a user agent/device; or

(b) data exposed by the use of network communications protocols.

There are many types of data that can form a fingerprint, including the following examples:

(a) CSS information;

[8] Sometimes referred to as the "Internet of Things"

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

[10] *Singling out*: the possibility to isolate some or all records which identify an individual in the dataset, Opinion 05/2014 on Anonymisation Techniques, pp 11-12.

[11] *Linkability*: the ability to link, at least, two records concerning the same data subject or a group of data subjects (either in the same database or in two different databases). If an attacker can establish (e.g. by means of correlation analysis) that two records are assigned to a same group of individuals but cannot single out individuals in this group, the technique provides resistance against "singling out" but not against linkability, Opinion 05/2014 on Anonymisation Techniques, pp 11-12.

[12] *Inference*: the possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes, Opinion 05/2014 on Anonymisation Techniques, pp 11-12.

(b) JavaScript objects (e.g., document, window, screen, navigator, date and language);

(c) HTTP header information (e.g., the number of bits of information in the User Agent string, HTTP header ordering, HTTP header variation by request type);

(d) clock information (e.g., clock skew and clock error);

(e) TCP stack variation;

(f) installed fonts;

(g) installed plugin information (e.g., configuration and version information);[13]

(h) the use of internal Application Programming Interfaces[14] (API) exposed by the user agent/device; or

(i) the use of external API's of Web services the user agent/device is communicating with.

4. Technical background

The internet and the Web have been developed with the needs of a resilient and open architecture network environment in mind.[15] Due to design choices to meet these needs, devices transmit information elements. A number of protocols include a range of mandatory and optional information elements. For example, the HTTP/1.1[16] protocol specifies header fields which allow the server and the client to include additional information regarding the hypertext. Some of these were specifically intended for the server to recognise client types. For example, the User-Agent request-header field includes the description: "*This is for statistical purposes, the tracing of protocol violations, and automated recognition of user agents for the sake of tailoring responses to avoid particular user agent limitations*".

Typical uses of the User Agent String include the optimisation of the layout of content for a particular type of device; to use this information to target content to specific users;[17] or to collect information about the device for security or analytics purposes.

5. Data protection risks

Because an individual HTTP header typically has a non-unique value, users can rarely be individually identified from the information element alone.[18] For example, the media types supported by a browser

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

[14] The API offers a user friendly framework for accessing functions or routines within a software component.

[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 Jorunal, 2012. On Orbitz, Mac Users Steered to Pricier Hotels, http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html

are often the same amongst many other users utilizing the same browser version. Therefore, when processed in isolation, these non-unique information elements do not generally present a data protection risk.

However, a number of information elements can be combined to provide a set which is sufficiently unique (especially when combined with other identifiers such as the originating IP address) to act as a unique fingerprint for the device or application instance. Such a fingerprint provides the ability to distinguish one device from another and can be used as a covert alternative for cookies to track internet behaviour over time.[19,20,21] As a result, an individual may be associated, and therefore identified, or made identifiable, by that device fingerprint.

The data protection risks of device fingerprinting are increased by the fact that the unique set of information elements is not only available to the website publisher, but also to many other third parties. This is in contrast to the *same origin* policy of HTTP cookies and exacerbated by the technical nature of the world wide web, where many third parties contribute to the content of a web page.

It is common that a single webpage is dynamically generated in real-time by requesting content from multiple sources. Each of these resources will generate HTTP requests of their own, downloading images, JavaScript and CSS files. Many webpages also contain web-bugs and tracking scripts. They may also issue HTTP requests that record when a user scrolls or clicks on a page, image or advertisement. Therefore, third-parties frequently have the opportunity to collect the information needed to fingerprint the user's device.

The data protection risks are not limited to tracking by third parties. The combination of data obtained through Application Programming Interfaces (API) present in the software on client devices also poses a risk of device fingerprinting. Different software, platforms and APIs will each offer access to different information elements stored in the device. The web browser JavaScript API, for example, can provide information relating to the screen size, colour depth and available system fonts. Other APIs may request access to information elements stored in the firmware (e.g. the CPU type), operating system (e.g. the OS type) or graphics card model.[22] API calls may also reveal the presence of installed software (e.g. browser plug-ins) or even the precise version numbers. Access to such sets of information increases the number of bits of information (entropy) and therefore the risk of recognition of unique individuals through their device.[23]

[18] There are cases where a single information element carries information that may uniquely identify a data subject, such as an OAuth access token.

[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

[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

In contrast to HTTP cookies, device fingerprinting can operate covertly.[24] There are no simple means for users to prevent the activity and there are limited opportunities available to reset or modify any information elements being used to generate the fingerprint. As a result, device fingerprints can be used by third-parties to secretly identify or single out users with the potential to target content or otherwise treat them differently.

It has been noted in Opinion 16/2011[25] that advertising companies have argued that the use of unique codes or other values does not involve the processing of personal data. This is in contradiction to the purpose of processing for the delivery of personalised content and advertisements, i.e., to communicate directly with a specific individual. The Working Party has argued on many occasions that such unique identifiers qualify as personal data.[26]

6. Legal framework

When a fingerprint is generated through the storage of or access to information stored in the user's terminal device, the ePrivacy Directive applies.

As described in Opinion 04/2012, Article 5(3) allows for processing to be exempt from the requirement of consent, if one of the following criteria is satisfied:

CRITERION A: technical storage or access "for the sole purpose of carrying out the transmission of a communication over an electronic communications network".

CRITERION B: technical storage or access which is "*strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*".

Furthermore, the website operator must respect the defined meaning of any other signal which indicates the user's preference in this regard - such as the Do-Not-Track[27] header.[28]

Although the application of the Data Protection Directive is outside the scope of this Opinion where device fingerprinting constitutes the processing of personal data it is important that this is done in accordance with each relevant provision of this Directive.

[24] Only in specific cases, the protocol requires a signal to the user, such as the geolocation HTML5 API specification. See: http://www.w3.org/TR/geolocation-API/#privacy_for_uas.

[25] Article 29 Working Party, 2014. Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf

[26] Article 29 Working Party, 2014. Opinion 05/2014 on Anonymisation Techniques, pp 11-12. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

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

[28] The Do Not Track protocol has potential, under certain circumstances, to become a granular consent mechanism that is in line with Recital 66 of Directive 2009/136/EC Recital allows for users to express consent through their browser settings, but only if the consent complies with the above mentioned requirements for valid consent. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140606_wp29_ts_standardisation_letter_to_w3c.pdf

Article 5(3) of the ePrivacy Directive sets the requirement for consent from the user for any party which intends to store or access information stored in the user's terminal device, even if that information is not yet considered to be personal data. WP29 has discussed consent in a number of opinions both in general[29] and with specific regard to online behavioural advertising.[30] The Working Party has also discussed the consent requirement in the context of Article 5(3) and cookies.[31]

It is worthy to recall Opinion 02/2013 on apps on smart devices[32] which noted:

"the distinction between the consent required to place any information on and read information from the device, and the consent necessary to have a legal ground for the processing of personal data. Though both consent requirements are simultaneously applicable [...] the two types of consent can be merged in practice, provided that the user is made unambiguously aware of what he is consenting to."

Recital 66 of the ePrivacy Directive refers to "*unwarranted intrusion into the private sphere*" and Article 5 addresses the requirement for the confidentiality of the communications. Article 5(3) can be regarded as extending the confidentiality of information to that which is stored or accessed on the user's device. Therefore any processing which the third-party undertakes which influences the behaviour of that device or otherwise cause it to store or give access to information on that device, or exposed by that device is within the scope of Article 5(3).

Use of the words "*stored or accessed*" indicates that the storage and access do not need to occur within the same communication and do not need to be performed by the same party. Information that is stored by one party (including information stored by the user or device manufacturer) which is later accessed by another party is therefore within the scope of Article 5(3). An example is a mobile phone app which processes the user's contact list where the contact details are stored by the user himself but the access is performed by the third-party. It is not correct to interpret this as meaning that the third-party does not require consent to access this information simply because he did not store it. The consent requirement also applies when a read-only value is accessed (e.g. requesting the MAC address of a network interface via the OS API).

Thus it is important for a third-party to remember that where device fingerprinting requires the storage of, or access to, (a set of) information on the user's device then consent will be required (unless a valid exemption applies). This will remain the case even if some of those information elements did not require the storage of, or access to, information.

7. Use case scenarios

[29] Article 29 Working Party, 2011. Opinion 15/2011 on the definition of consent. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

[30] Article 29 Working Party, 2010. Opinion 2/2010 on online behavioural advertising. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

[31] Article 29 Working Party, 2013. Working Document 02/2013 providing guidance on obtaining consent for cookies. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

[32] Article 29 Working Party, 2013. Opinion 02/2013 on apps on smart devices. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

7.1. Use case: First-party website analytics

A number of online services have proposed device fingerprinting as an alternative to HTTP cookies for the purpose of providing analytics without the need for consent under Article 5(3). In Opinion 04/2012 the Working Party recognised the need for a third exemption for the consent requirement for first party analytics:

"*provided that they are strictly limited to first party aggregated statistical purposes and when they are used by websites that already provide clear information about these cookies in their privacy policy as well as adequate privacy safeguards. Such safeguards are expected to include a user friendly mechanism to opt-out from any data collection and comprehensive anonymization mechanisms that are applied to other collected identifiable information such as IP addresses.*"

However, the Opinion also stated that currently there is no exemption to consent for cookies that are strictly limited to first party anonymised and aggregated statistical purposes.[33] Therefore, first-party website analytics through device fingerprinting do not fall under the exemption defined in CRITERION A or B and consent of the user is required.

7.2. Use case: Tracking for online behavioural advertising

Many websites include third-party web-bugs, pixel tags and JavaScript code to enable advertising services. This results in a number of requests for information elements from the user's device. The requests are transmitted to the third-parties providing the advertising services, and allow them to generate a device fingerprint to follow users across websites and over time, and create an interest profile for targeted advertising, even if the user declines cookies. Such processing can technically be undertaken in a covert manner without the knowledge of the user.

Opinion 04/2012 emphasised that third-party advertising does not fall under the exemption defined in CRITERION A or B. Therefore, device fingerprinting for the purpose of targeted advertising requires the consent of the user.

7.3. Use case: Network provision

The correct management of a network requires the transfer of certain information elements relating to each device on the network. For example, a Wi-Fi access point which manages the connection between wireless devices and a wired network will process unique and non-unique information elements such as the MAC address[34] and channel in order to correctly maintain connections and correctly route data packets.

Where the network provisioning requires information elements which store or gain access to information on the user's device then this will fall within scope of Article 5(3). Where this processing is required for the normal functioning of the network, then this would be exempt under CRITERION A.

[33] Article 29 Working Party, 2012. Opinion 04/2012 on Cookie Consent Exemption, pp. 10-11.

[34] The MAC address will likely be unique across devices on the network. The MAC address prefix will refer also to the chip manufacturer.

The secondary use of an information element or device fingerprint for the purpose of tracking is not considered as "*for the sole purpose of carrying out the transmission of a communication over an electronic communications network*" or "*strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*". When considering multi-purpose cookies in Opinion 04/2012, WP29 noted that "*tracking is very unlikely to meet CRITERION A or B"* thus if a third-party wishes to use a device fingerprint for multiple purposes it will only be "*exempted from consent if all the distinct purposes [...] are individually exempted from consent*".

7.4. Use case: User access and control

An online service may intend to use device fingerprinting to support user access and control (i.e. in combination with a username and password). The device fingerprint can be used to ensure that an account is linked to a particular device such that the device acts as a second factor of authentication.

For example, a music subscription service only permits a user to access the service from a limited number of specific devices. If a user has used this device previously, the website operator can choose to perform fewer verification checks before providing access.

If a device fingerprint is comprised of information elements which store or gain access to information on the user's device then this will fall within the scope of Article 5(3). Such purposes would however not be considered as "*strictly necessary"* to provide a functionality explicitly requested by the user and therefore valid user consent is required.

Website operators may need to consider a range of appropriate and proportionate controls or any other authentication method (e.g. a one-time password, secondary email confirmation).

7.5. Use case: User centric security

In Opinion 04/2012, WP29 stated that "*cookies set for the specific task of increasing security of the service that has been explicitly requested by the user"* (e.g. to detect repeated failed login attempts) would be exempt under CRITERION B.

This exemption would also apply to device fingerprinting but, as with cookies, "*not [...] cover the use of the technique that relate to the security of websites or third party services that have not been explicitly requested by the user.*"

If data are collected via device fingerprinting to serve a user centric security purpose, in order to qualify for the consent exemption, they may not be used for any secondary purposes. Technical and organisational safeguards must be taken to prevent any secondary use of finger printing data, typically kept in server security logs.

7.6. Use case: Adapting the user interface to the device

Accessing device information such as the screen size can be useful to optimise the layout of content.[35] For example, a media website could switch to a low graphics mode or single column layout for mobile

[35] Note that other less privacy instructive methods may exist to achieve this same objective such as using the User-Agent string.

devices. Alternatively a website, or the third-parties serving content through that website, might query the device to ascertain technical capabilities such as which video formats are supported.

Where a third-party requests access to information stored on the user's device for the sole purpose of adapting the content to the characteristics of the device, then CRITERION B is valid. This means that for short-term UI customisation consent is therefore not required.

If this information however is also used for secondary purposes, this exemption no longer applies.

8. Conclusion

This Opinion addresses the topic of device fingerprinting and the applicability of Article 5(3) of the ePrivacy Directive 2002/58/EC, as amended by Directive 2009/136/EC, without prejudice to the provisions of the Data Protection Directive 95/46/EC. This Opinion expands upon the earlier Opinion 04/2012 on Cookie Consent Exemption and confirms that, in a number of circumstances, the technology leads to the gaining of access to, or storing of, information on the user's terminal device. Thus Article 5(3) of the ePrivacy Directive also applies to instances of device fingerprinting.

Therefore, parties who wish to process device fingerprints which are generated through the gaining of access to, or the storing of, information on the user's terminal device must first obtain the valid consent of the user (unless an exemption applies).