Web Tracking meets Data Privacy (Part 1)

German Telemedia Act and GDPR[1]

Dr. Jörg Kaufmann, Lawyer, Schadbach Rechtsanwälte

Trackers use a number of different methods, such as browser cookies, fingerprints, IP-addresses and so forth, to track the behaviour of Internet users. They collect data on users and aggregate them into profiles, which can then be used as a basis for targeted advertising. Before the GDPR became applicable on 25 May 2018, sec. 15 para. 3 German Telemedia Act allowed providers of telemedia services to create pseudonymous user profiles for the purpose of advertising, market research or the adequate implementation of telemedia services. However, since 25 May 2018, the data privacy provisions in the German Telemedia Act are no longer applicable. As the ePrivacy Regulation is still under discussion, the lawfulness of online data processing is currently governed only by the GDPR.

1

This two-part essay examines the technical background of web tracking (Part 1) as well as its legal implications by considering its legal status before and after the GDPR (Part 2). Important to this examination is the ongoing discussion about the requirement of the user's consent (opt-in) as opposed to the user's right to object to the processing of personal data (opt-out). There is, however, no practical value to a consent declaration that is given online. Moreover, web tracking and data privacy law are difficult to reconcile; data protection authorities are critical of third-party and cross-device web tracking.

2

I. Introduction

The term *tracking* refers to methods that enable the recognition of Internet users and the facilitation of their online user activity analysis over a long period of time, specifically in order to assign personal attributes to those users.[2] Spending behaviour, personal interests, political attitude, approximate age, family status and so forth can be distilled

3

---

[1] This essay was written while the author was partner at WALDENBERGER RECHTSANWÄLTE, Berlin.

[2] *Hanloser*, ZD 2018, 213.

from these online activities[3] and thus saved in user profiles.[4] The main purpose of tracking is to prepare a data basis for targeted advertising.[5] However, the analysis of data collected by web tracking may serve other purposes as well. For example, the provision of information services and credit scoring can be based on web tracking as well.[6]

Web analytics and web tracking are two closely related fields.[7] In some cases web analytics is even considered a sub-element of web tracking.[8] Web analytics[9] refers to the collection, measurement, analysis and presentation of Internet data for the purpose of understanding and optimising the use of websites.[10] The analysed data may include device type, language settings, region, location and user activity.[11] A comprehensive user profiling is not required for the statistical purpose of web analytics. Web analytics focuses more on the performance of a website,[12] whereas web tracking targets the Internet user.[13]

4

II. Technical Background

A distinction can be made between two classes of tracking methods.[14] Firstly, trackers transfer and save data onto the terminal equipment of Internet users by using web cookies, flash cookies, eTags, local storage and so forth. This saved information can later be used to recognise either the user or his/her browsing device. Secondly, trackers use a combination of configuration details and system properties of users' devices for the purpose of user recognition, for example in browser fingerprinting and IP-address-tracking.[15] Trackers are not restricted to the use of one particular form of tracking but take advantage of different tracking methods at the same time. This technical flexibility enhances the performance of web tracking by placing restrictions on the user's attempts to counter tracking.

5

---

[3] *Schneider/Enzmann/Stopczynski*, Frauenhofer SIT, Web Tracking-Report 2014, 7, https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2 014.pdf, (all websites last accessed on July 15, 2019).

[4] *Schleipfer*, ZD 2017, 460.

[5] *Schmücker*, Web Tracking, 2011, 1, http://www.snet.tu-berlin.de/fileadmin/fg220/courses/SS11/snet-project/web-tracking_schmuecker.pdf.

[6] *Schneider/Enzmann/Stopczynski*, Frauenhofer SIT, Web Tracking-Report 2014, 8, https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2 014.pdf.

[7] *Schmücker*, Web Tracking, 2011, 1, http://www.snet.tu-berlin.de/fileadmin/fg220/courses/SS11/snet-project/web-tracking_schmuecker.pdf.

[8] *Härting*, Internetrecht, 6th edition 2017, Datenschutzrecht, rec. 232.

[9] Examples of web analytics tools are *Google Analytics*, *Adobe Analytics* and *Matomo*.

[10] *AT Internet*, Glossary Web Analytics, https://www.atinternet.com/en/glossary/web-analytics-2/.

[11] *Schwartmann/Benedikt/Jacquemain*, PinG 2018, 150, 154.

[12] *Schleipfer*, ZD 2017, 460, 461.

[13] *Schirmbacher*, ITRB 2016, 274, 278.

[14] *Schneider/Enzmann/Stopczynski*, Frauenhofer SIT, Web Tracking-Report 2014, 9, https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2 014.pdf.

[15] *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, 49.

1. Web Cookies

Web cookies are still the most widely used tracking method.[16] A cookie is a small text file that usually contains an identification number.[17] The file is saved on the device of the Internet user upon his/her visit to a particular website. If the user visits the website again, his/her device can be recognised by reading the cookie.[18] Moreover, aspects such as time spent on the website, language settings and login status can be tracked by the use of cookies. Internet users may choose, however, to reject or delete cookies in their browser settings.

6

A first-party cookie is set by a website whose domain the Internet user has directly accessed.[19] This type of cookie is usually generated for the purpose of analytics or functionality. In contrast, third-party cookies are generated by websites whose domain the user has not intentionally accessed. Third-party websites supply additional data such as images and scripts in advertising banners.[20] The third-party tracking scenario is based on two technical prerequisites.[21] Each time a user visits a particular website, a connection to the tracker has to be established in order to inform the tracker about the visits to the website. In addition, the tracker has to be able to make a connection between various website visits and a particular user. In order to fulfill these two requirements, certain code elements have to be embedded into the website.

7

Advertising networks such as AdKlick and DoubleClick aggregate advertising content from advertisers and then establish a connection to publishers who will display the advertising content on their websites.[22] The network sets up a user profile which is connected to the third-party cookie saved on the user's device.[23] Each time the Internet user visits a website into which the code of the advertising network has been embedded, his/her device will be recognised by reading the cookie. The advertising network can use the data saved in the user profile to deliver customised advertisements to the Internet user.[24]

8

---

[16] *Hanloser*, ZD 2018, 213.

[17] *Härting*, Internetrecht, 6th edition 2017, Datenschutzrecht, rec. 223.

[18] *Lotze/Heinson/Hasselblatt*, MAH Gewerblicher Rechtsschutz, 5th edition 2017, sec. 30, rec. 102.

[19] *Bauer* et al., BVDW-Whitepaper, Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte, 2015, 6, https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/data_economy/whitepaper_targeting_browsercookies-und-alternative-trackingtechnologien_2015.pdf.

[20] *Schmücker*, Web Tracking, 2011, 4, http://www.snet.tu-berlin.de/fileadmin/fg220/courses/SS11/snet-project/web-tracking_schmuecker.pdf.

[21] *Schneider/Enzmann/Stopczynski*, Frauenhofer SIT, Web Tracking-Report 2014, 8, https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2014.pdf.

[22] *Schmücker*, Web Tracking, 2011, 3, http://www.snet.tu-berlin.de/fileadmin/fg220/courses/SS11/snet-project/web-tracking_schmuecker.pdf.

[23] *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, 59.

[24] *Schleipfer*, ZD 2017, 460, 461.

2. Flash Cookies

Adobe Flash Player is a browser plugin used primarily for animated and interactive content.[25] This plugin saves flash cookies on the user's device.[26] They are not tied to a specific browser, thus enabling the identification of users across different browsers.[27] Flash cookies can be managed/deleted only in the flash player settings manager.[28]

9

3. Local Storage

Web cookies have only a small storage capacity and the saved information is transferred with every HTTP-request. In contrast, local storage offers the possibility of saving large amounts of data in the user's web browser.[29] Moreover, the saved information does not have to be sent back and forth with every HTTP-request. Local storage can also save a specific user-ID, which makes it a very effective tracking method. The deactivation of JavaScript prevents local storage but also affects the functionality of many websites.[30] Alternatively, the Internet user may manually delete the browser's cache to remove the saved data.

10

4. eTag

Communication between browser and server is based on a request by the browser to the server and a corresponding response by the server to the browser.[31] Both request and response consist of two parts: the data to be transferred and a header with additional metadata. The entity tag (eTag) is a field in the header of request and response that will be used for browser caching. Web servers use eTags to compare resources and determine

11

---

[25] *Schmücker*, Web Tracking, 2011, 4, http://www.snet.tu-berlin.de/fileadmin/fg220/courses/SS11/snet-project/web-tracking_schmuecker.pdf.

[26] *Lotze/Heinson/Hasselblatt*, MAH Gewerblicher Rechtsschutz, 5th edition 2017, sec. 30, rec. 103.

[27] *Alich/Voigt*, CR 2012, 344, 345.

[28] *Bauer* et al., BVDW-Whitepaper, Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte, 2015, 20, https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/data_economy/whitepaper_targeting_browsercookies-und-alternative-trackingtechnologien_2015.pdf.

[29] *Bauer* et al., BVDW-Whitepaper, Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte, 2015, 18, https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/data_economy/whitepaper_targeting_browsercookies-und-alternative-trackingtechnologien_2015.pdf.

[30] *Schmücker*, Web Tracking, 2011, 4, http://www.snet.tu-berlin.de/fileadmin/fg220/courses/SS11/snet-project/web-tracking_schmuecker.pdf.

[31] *Bauer* et al., BVDW-Whitepaper, Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte, 2015, 16, https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/data_economy/whitepaper_targeting_browsercookies-und-alternative-trackingtechnologien_2015.pdf.

whether they are identical or not.[32] If the checksums are identical, the resource requested by the web browser will not be loaded from the server, but rather from the browser's cache. Many websites use eTags for tracking purposes. The Internet user may, however, delete the browsers' cache to avoid being tracked with eTags.

5. IP-Address-Tracking

An Internet Protocol Address (IP-address) is a logical numeric address that is assigned to every single device connected to the Internet. There are static and dynamic IP-addresses.[33] The IP-address can be used to determine the approximate location of the user's device and the name of the access provider.[34] Trackers usually save the IP-address of the device together with the time of the Internet access and further data such as the used data volume.[35] There are certain limitations in IP-address-tracking. For example, the IP-address of the device may change after a while or one IP-address might be shared by several users.[36] In addition, the Internet user may take advantage of anonymiser proxies to conceal the IP-address of his/her device.

12

6. Browser Fingerprinting

The term fingerprinting refers to procedures that recognise the devices of Internet users with a combination of hard- and software features.[37] Combinations such as device type, operating system, browser extensions, character encoding, language, time zone and so forth constitute an almost unique browser ID.[38]

13

There is active and passive fingerprinting.[39] Active fingerprinting refers to information that is collected by JavaScript, for example, operating system, time zone, font size and resolution. Passive fingerprinting refers to the process of automatically transferring information from the user's device to the server, such as IP-address and browser type.

14

---

[32] *Brinkmann*, A solution to ETAg tracking in Firefox, 2017, https://www.ghacks.net/2017/12/09/a-solution-to-etag-tracking-in-firefox.

[33] *Härting*, Internetrecht, 6th edition 2017, Datenschutzrecht, rec. 230.

[34] *Maisch*, ITRB 2011, 13, 14.

[35] *Schürmann*, DSB 2017, 9, 10.

[36] *Schneider/Enzmann/Stopczynski*, Frauenhofer SIT, Web Tracking-Report 2014, 44, https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2014.pdf.

[37] *Bauer* et al., BVDW-Whitepaper, Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte, 2015, 13, https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/data_economy/whitepaper_targeting_browsercookies-und-alternative-trackingtechnologien_2015.pdf.

[38] *Maisch*, ITRB 2011, 13, 16; *Mayer/Mitchell*, Third-Party Web Tracking, Policy and Technology, 2012, 421, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6234427.

[39] *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, 65.

With the use of browser fingerprinting, a device can therefore be tracked across different websites.

The information that is collected by fingerprinting is stored on the server and not on the device of the user.[40] The information cannot therefore be deleted without the operator of the server. The deactivation of JavaScript affects not only browser fingerprinting but also the usability of many websites. Alternatively, the Internet user can install browser plugins to block the script.[41] This procedure does not stop fingerprinting altogether, although it does prevent the creation of a unique device ID.

15

7. ID-Tracking

Social networks, webmail providers, streaming services and e-commerce shops are all internet services that require users to register and log in. As such, they can take advantage of ID-tracking.[42] The Internet service assigns to each of its users a unique ID that contains all relevant user data. The purpose of ID-tracking is to identify a particular Internet user and not a browser or device. This form of tracking does not work if the Internet user signs out of his/her account or opens the website in a different browser.

16

The login details for accounts with service providers such as Facebook, Google, and Twitter can be used for authentication on other websites as well. For example, Facebook members may use their profile to log onto websites that accept Facebook Connect.[43] In this scenario, there is no need for the Facebook user to set up a separate account for the service of the third-party website.[44] During the login process, the third party will get access to certain personal data of the Facebook user, such as full name, profile picture, age and friend list.

17

The Share/Like buttons of social networks such as Facebook and Twitter can be integrated into third-party websites. If Internet users klick on these buttons, the content will be shared with their followers on Facebook and Twitter.[45] The Share/Like function only works if the user is logged in to the social network. Accordingly, the social network can identify

18

---

[40] *Bauer* et al., BVDW-Whitepaper, Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte, 2015, 14,
https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/data_economy/whitepaper_targeting_browsercookies-und-alternative-trackingtechnologien_2015.pdf.

[41] *Schanze*, Browser-Fingerprint – Was ist das? Wie verhindern?, 2018,
https://www.giga.de/extra/ratgeber/specials/browser-fingerprint-was-ist-das-wie-verhindern-einfach-erklaert.

[42] *Bauer* et al., BVDW-Whitepaper, Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte, 2015, 16,
https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/data_economy/whitepaper_targeting_browsercookies-und-alternative-trackingtechnologien_2015.pdf.

[43] *XOVI Handbuch*, Facebook Connect, https://www.xovi.de/wiki/Facebook_Connect.

[44] *RYTE WIKI*, Facebook Connect, https://de.ryte.com/wiki/Facebook_Connect.

[45] *Maisch*, ITRB 2011, 13, 15.

its member and the websites that have been visited. The operator of the third-party website will then be informed by the social network about the user's identity.[46]

8. Mobile Advertising-IDs

The functionality of cookies on mobile devices is limited. Advertisers therefore employ mobile advertising-IDs to track users.[47] This type of ID is a resettable identifier that can be found on almost every mobile device. The purpose of the advertising-ID is to enable targeted advertising vis-à-vis the app user. The resettable character of the mobile advertising-ID is a significant difference to past forms of mobile advertising that relied on fixed Unique Device Identifiers.[48]

19

9. Bottom Line

Web tracking is a phenomenon which affects all Internet users. The online advertising industry employs a wide array of highly effective tracking methods for the purpose of aggregating as much information as possible on Internet users. Web tracking is often considered an invasion of users' privacy. Yet it is nevertheless important to keep some basic facts in mind. Users prefer Internet services to be free.[49] Facebook, Google, Twitter, and Instagram would not be able to operate without millions of Internet users who share their personal data with these service providers. Furthermore, web tracking operates as only one aspect of the modern surveillance state. The deletion or delimitation of web tracking will not necessarily impact on other forms of surveillance and data collection that permeate the fabric of modern society. In addition to computers, tablets, smartphones and social media, data is also collected on a daily basis from other technologies, such as smart cars, smart homes, fitness trackers, electronic payment transactions and surveillance systems.[50]

20

---

[46] *Bauer* et al., BVDW-Whitepaper, Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte, 2015, 16,
https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/data_economy/whitepaper_targeting_browsercookies-und-alternative-trackingtechnologien_2015.pdf.
[47] *Hanloser*, ZD 2018, 213, 214.
[48] *Bauer* et al., BVDW-Whitepaper, Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte, 2015, 22,
https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/data_economy/whitepaper_targeting_browsercookies-und-alternative-trackingtechnologien_2015.pdf.
[49] *Härting*, Internetrecht, 6th edition 2017, Datenschutzrecht, rec. 217.
[50] *Schürmann*, DSB 2017, 9.