

Like or Dislike—Web Tracking

Charlotte Röttgen

Abstract Web tracking enables recording and analysis of user behavior and comes along in various manifestations. The use of cookies and social-plugins on websites, for instance, allows identifying how often a user visits a concrete website and which content he or she is interested in. Through this, companies “decode” the user behind its data and are able to provide targeted advertising. Even though web tracking may not be prevented entirely, different possibilities do exist to limit user analysis.

1 Web Tracking—A Definition

It frequently occurs that astonishment sets in about upcoming advertisement while surfing the internet. By pure chance, the advertised products match those products users are interested in for quite some time. But how does the linking of information work, which occurs, for instance, in case of “targeted advertising”? The answer is: by web tracking.

By using web tracking a webmaster gets to know inter alia the user behavior on his website, from which website users enter the webmaster’s site, how long they stay on it and how often they visit the site.¹ Additionally, location data and content from email communication can be tracked. Evaluating this multitude of users’ data tracks, the webmaster is able to create tracking profiles. These profiles contain statements based on probabilities about interests, political persuasion, level of education, and even the sexual orientation of the visitors. This is valuable information, since it enables highly targeted advertising.

¹Bouhs, Der gläserne Internetnutzer, Deutschlandfunk.de, http://www.deutschlandfunk.de/datenerfassung-der-glaeserne-internetnutzer.761.de.html?dram:article_id=293516.

C. Röttgen (✉)
Institute for Information, Telecommunication and Media Law (ITM),
University of Münster, Münster, Germany
e-mail: charlotte.roettgen@uni-muenster.de

In general, the more they know about the customers' interests and wishes, the more accurately advertising targeting can be and the more likely it is that customers buy the advertised products.

2 What Types of Web Tracking Technologies Exist?

There are various types of web tracking technologies. In view of the large number of tracking methods, only some of them are exemplified below.

Cookies are one classical tracking tool: small text files stored in the user's browser, assigning information about the site he came from—for example, he clicked on an advertising banner on another website—the frequency of visits and his behavior on the website.² Not all types of cookies should be regarded with mistrust. What they all have in common is the recognition of a browser, respectively, of a user. The essential question in this context is: who set the cookie and with what intention?

The cookie set by a webmaster once the visitor loaded the website primarily, simplifies the visit of the website.³ The browser's recognition by cookies enables a faster loading of the website. If the website provides authentication, further login is expendable. *Third party cookies*, however, allow cross-website tracking through all websites, on which they are placed.⁴

So-called *zombie cookies* are a persistent type of tracking cookies, which cannot be deleted easily. They are stored in the browser several times and on different ways. Deleting one type of cookie is detected by the other cookie files and enables auto recovery of the deleted one.

Furthermore, another method which is normally combined with tracking cookies is *embedding content on foreign websites with social plugins* by Facebook or other social media platforms.⁵ Facebook, for example, places the "Like-Button" on various websites. In combination with cookies, tracking the user's behavior (so-called coverage analysis/web analytics) is possible even if the user already left the Facebook Website or has not visited Facebook before.

It is also possible to recognize and locate a user by the *IP address* of his device which is transmitted to the server with each visit of a website.⁶ An approximate

²Mauerer, Web Privacy, Seminar Future Internet, Network Architectures and Services, p 26, https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2015-09-1/NET-2015-09-1_04.pdf.

³Mauerer, Web Privacy, Seminar Future Internet, Network Architectures and Services, p 26, https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2015-09-1/NET-2015-09-1_04.pdf.

⁴Schallaböck 2014a, Verbraucher-Tracking, p 21, https://www.gruene-bundestag.de/fileadmin/media/gruenebundestag_de/themen_az/digitale_buengerrechte/Tracking-Bilder/Verbraucher_Tracking.pdf; Schneider/Enzmann/Stopczynski, Web-Tracking-Report 2014, p 7, https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2014.pdf.

⁵Lotz, E-Commerce und Datenschutzrecht im Konflikt, p 199.

⁶Lotz, E-Commerce und Datenschutzrecht im Konflikt, p 196 et seqq.

localization is possible, because most regions allocated a special range of IP addresses.⁷

Another tracking tool is *canvas fingerprinting*. It allows webmasters to recognize the user's digital fingerprint by analyzing browser settings, transmitted with every page view (including browser version, installed browser add-ons, operating system, screen definition and more).⁸ Combining these with other information an extensive profile of the user can be generated.

By analyzing Email content to certain signal words it is able to detect interests and needs of the user. As a result, improved targeted advertising—so called *E-Mail tracking*—is provided. This affects, for example, users with Gmail accounts.⁹

Through the establishment of smartphones and tablets web tracking achieved a new level of user analysis. *App Tracking* allows a cross-application identification of the user.¹⁰ Depending both on the apps that are installed as well as how (or not) the user configured his smartphone, location data, surfing behavior and other information is recorded. Those apps, which record location data and allow extensive analysis, are, regardless of the service offered, often for free. There are considerable doubts that these apps are for free, actually—understanding “free” as a service without consideration. The user “pays” by the disclosure of his data.

Tracking by recording users' keystrokes while surfing online, a new method from the field of behavior analysis is still in its infancy.¹¹ Special software¹² can identify users by their input speed, key press and writing behavior. According to the company BehavioSec, in a test phase 99% of users has been identified.¹³

The companies, that use tracking tools described above, can profit by considerably expanded range of user tracking (so called cross-domain-tracking). A greater

⁷Schallaböck 2014b, Was ist und wie funktioniert Webtracking?, <https://irights.info/artikel/was-ist-und-wie-funktioniert-webtracking/23386>; Schultzi-Haddouti, Ein bisschen Datenschutz ist schon eingebaut, FAZ.net, <http://www.faz.net/aktuell/technik-motor/computer-internet/privatsphaere-und-tracking-ein-bisschen-datenschutz-ist-schon-gebaut-13838753.html>.

⁸Maurer, Web Privacy, Seminar Future Internet, Network Architectures and Services, p 27, https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2015-09-1/NET-2015-09-1_04.pdf.

⁹Schallaböck 2014b, Was ist und wie funktioniert Webtracking?, <https://irights.info/artikel/was-ist-und-wie-funktioniert-webtracking/23386>.

¹⁰Schallaböck 2014b, Was ist und wie funktioniert Webtracking?, <https://irights.info/artikel/was-ist-und-wie-funktioniert-webtracking/23386>; Schneider/Enzmann/Stopczynski, Web-Tracking-Report 2014, p 53, https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2014.pdf; Schonschek 2014, App-Tracking: Was Apps alles verraten, <https://www.datenschutz-praxis.de/fachartikel/app-tracking-apps-alles-verraten/>.

¹¹Datenschutzbeauftragter-Info.de 2015, Neue Tracking-Methoden: Tastatur-Eingaben und Akku-Ladestand, available at: <https://www.datenschutzbeauftragter-info.de/neue-tracking-methoden-tastatur-eingaben-und-akku-ladestand/>.

¹²Companies like KeyTrack or BehavioSec provide software, which can identify users by their keystroke.

¹³Olsen Olson 2014, Forget Passwords. Now Banks Can Track Your Typing Behaviour On Phones, <https://www.forbes.com/sites/parmyolson/2014/08/18/forget-passwords-now-banks-can-track-your-typing-behavior-on-phones/#e1b3a7554de8>.

range of cross-domain tracking raises not only the quantity of the data used to create user profiles but also—and this is a crucial point—the quality of the data. This results in a holistic mosaic of the respective user.

3 How to Avoid Being Tracked

There are several ways in which tracking can be limited—but you cannot prevent it entirely. Users can change their browser settings, delete cookies manually or install browser add-ons like Adblock or Ghostery.

Later browser versions provide a preinstalled privacy mode with integrated tracking prevention. By activating this mode, all blacklisted trackers are blocked.

Furthermore, an interesting approach for the prevention of web tracking developed by German company eBlocker is using hardware directly connected at the WLAN access point.¹⁴ The advantage of this anti-tracking technology is the protection of all devices connected to the wireless network.

Even deactivating JavaScript in the browser is a way to prevent cookies from being stored in the browser or at least to reduce the stored cookies. In newer browser versions, it is not easy to disable it manually, sometimes you need browser add-ons or you need to change the core settings of the browser.

One disadvantage of such protections is that many sites cannot be visited anymore or with restricted functionality only.

4 The Example of Facebook

The connection of different tracking technologies, especially cookies and social plugins, and the technologies' explosiveness for data protection is shown at the example of Facebook.

Web tracking practice of Facebook runs by implementing the “Like” button on various websites and the use of cookies—especially the *Datr-Cookies*, which upsets German data protectionists for years.¹⁵

This cookie is linked to the “Like” button and is stored in the browsers of all users visiting websites with the “Like” button implemented. It does not matter if the

¹⁴Ansorge/Pimpl 2015, Online advertising is rife with mistrust, Horizont.net, <http://www.horizont.net/medien/nachrichten/Mozilla-Online-advertising-is-rife-with-mistrust-137450>.

¹⁵Cf. Karg/Thomsen 2012, p 729 et seq.; Sueddeutsche.de, Datenschützer: Facebook hat keinen Respekt vor Privatsphäre, <http://www.sueddeutsche.de/digital/tracking-datenschuetzer-facebook-hat-keinen-respekt-vor-privatsphaere-1.2483240>; ULD, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, p 23 et seq., <https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf>. The Independent Centre for Privacy Protection Schleswig-Holstein already complained the data protection issues of the “Like”-button in 2011.

user pressed the button or—and this is explosive from the perspective of data protection—if the user is registered at Facebook.¹⁶ This cookie allows recognition every time visiting a Facebook fan page¹⁷ or website with Facebook “Like” plugin.¹⁸

The fact Facebook tracks also non-members without consent in data processing has moved Belgian and French data protection authority to take action in the recent past. Under current EU law the user’s consent¹⁹ in data processing is required in these cases.

In 2015 Belgian data protection authority sued Facebook (Belgian Privacy Commission 2015) for omission of the procedure described above. The authority threatened a fine of 250,000 € for each day on which Facebook continued its tracking practices, which in the opinion of the authority violate data protection law. In the court of first instance, the applicant won, but Facebook appealed against it, already.²⁰

In France, the data protection authority set Facebook a deadline to end the tracking of non-members without their consent.²¹

For the question if web tracking by using these technologies violates data protection law, it is crucial, if the tracked data is *personal data*. Whether IP addresses are personal data is discussed in literature and case law, for a long time.²² German Federal Court (BGH) requested the European Court of Justice (ECJ) in 2015 to give

¹⁶Acar et al. 2015, Technical Report for the Belgian Privacy Commission, p 5 et seq., https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf.

¹⁷Facebook fan pages are public and mostly created by companies, associations and institutions to complement or replace the own website to tell users about itself and contact them.

¹⁸According to the report of the Belgian Data Protection Authority the Datr-Cookie is stored only in the browsers of non-members if they visit a Facebook URL. This cookie is requirement for recognition by social plugins.

¹⁹In German Law the consent is regulated in sections 4, 4a Federal Data Protection Act (BDSG).

²⁰Gibbs 2016, Facebook wins appeal against Belgian privacy watchdog over tracking, the-guardian.com, <https://www.theguardian.com/technology/2016/jun/30/facebook-wins-appeal-against-belgian-privacy-watchdog-over-tracking>. The court of appeal dismissed the action on the ground that the Belgian Privacy Commission does not have the authority to regulate Facebook because its European base of operations is in Dublin.

²¹Untersinger, Données personnelles: le virulent réquisitoire de la CNIL contre Facebook, LeMonde.fr, http://www.lemonde.fr/pixels/article/2016/02/09/donnees-personnelles-le-virulent-requisitoire-de-la-cnil-contre-facebook_4861621_4408996.html; Sueddeutsche.de, Französische Datenschützer werfen Facebook Gesetzesverstöße vor, <http://www.sueddeutsche.de/news/service/internet-franzoesische-datenschuetzer-werfen-facebook-gesetzesverstoesse-vor-dpa.urn-newsml-dpa-com-20090101-160209-99-585875>.

²²Cf. BGH MMR 2011, p 341 et seq.; Schaar, Datenschutz im Internet, 2002; Eckhardt, CR 2011, p 339 et seq.; Hoeren, ZD 2011, p 3.

a ruling thereon.²³ Its decision could have extensive implications for the current tracking practice and its legal assessment.²⁴

5 Summary and Outlook

The web tracking technologies described above exemplarily confirm the thesis of data as the “new oil”. Because of the parties’ commercial interests (webmasters, marketing companies and others) it is no surprise advertisement is the important source of financing websites.

To this, the increasing tendency of Internet users to prevent ads and tracking by using ad blockers or other technologies is diametrically opposed.

There is growing evidence that, in order to fulfill the economic potential also in future, internet industry will respond, and will develop new technologies.

For example, Germany’s highest-circulation newspaper blocks its website for users with activated ad blockers. Who wants to enjoy the free content, should pay at least in the form of advertising. Other newspapers will follow probably. Newspapers abroad implemented already similar mechanisms. What technical developments are coming and how the jurisdiction will react on that—only the future will tell.

References

- Acar G, van Alsenoy B, Piessens F, Diaz C, Preneel B (2015) Facebook tracking through social plug-ins. Technical Report for the Belgian Privacy Commission. https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf. Accessed 4 Apr 2017
- Ansoorge K, Pimpl R (2015) Online advertising is rife with mistrust. Interview. <http://www.horizont.net/medien/nachrichten/Mozilla-Online-advertising-is-rife-with-mistrust-137450>. Accessed 4 Apr 2017
- Belgian Privacy Commission (2015) The judgement in the Facebook case. <https://www.privacycommission.be/en/news/judgment-facebook-case>. Accessed 4 Apr 2017
- BGH (2015) ECJ-request on storing dynamic IP addresses. GRUR 117(2):192–196
- BGH (2011) Storing dynamic IP addresses. MMR 14(5):341–364
- Datenschutzbeauftragter-Info.de (2015) Neue Tracking-Methoden: Tastatur-Eingaben und Akku-Ladestand. <https://www.datenschutzbeauftragter-info.de/neue-tracking-methoden-tastatur-eingaben-und-akku-ladestand/>. Accessed 4 Apr 2017
- Eckhardt J (2011) IP-Adresse als personenbezogenes Datum—neues Öl ins Feuer. CR 27(5): 339–344

²³Schleipfer, ZD 2015, p 399 et seq.

²⁴According to the opinion (case C 582/14) of Advocate General *Sánchez-Bordona* of the ECJ of May 2016 dynamic IP addresses must be classified as personal data. However, it is not yet clear whether the ECJ will follow this opinion.

- Gibbs S (2016) Facebook wins appeal against Belgian privacy watchdog over tracking. TheGuardian.com. <https://www.theguardian.com/technology/2016/jun/30/facebook-wins-appeal-against-belgian-privacy-watchdog-over-tracking>. Accessed 4 Apr 2017
- Hoeren T (2011) Google Analytics—datenschutzrechtlich unbedenklich? ZD 1(1):3–6
- Karg M, Thomsen S (2012) Tracking und Analyse durch Facebook—das Ende der Unschuld. DuD 36(10):729–736
- Untersinger M (2016) Données personnelles: le virulent réquisitoire de la CNIL contre Facebook. LeMonde.fr. http://www.lemonde.fr/pixels/article/2016/02/09/donnees-personnelles-le-virulent-requisitoire-de-la-cnil-contre-facebook_4861621_4408996.html. Accessed 4 Apr 2017
- Olson P (2014) Forget passwords. Now banks can track your typing behavior on phones. Forbes.com. <http://www.forbes.com/sites/parmyolson/2014/08/18/forget-passwords-now-banks-can-track-your-typing-behavior-on-phones/#33225a8b44cc>. Accessed 4 Apr 2017
- Schaar P (2002) Datenschutz im Internet. C. H Beck, München
- Schallaböck J (2014) Verbraucher-Tracking. Kurzgutachten. iRights.Law. http://www.gruenebundestag.de/fileadmin/media/gruenebundestag_de/themen_az/digitale_buergerrechte/Tracking-Bilder/Verbraucher_Tracking.pdf. Accessed 4 Apr 2017
- Schallaböck J (2014) Was ist und wie funktioniert Webtracking? <https://irights.info/artikel/was-ist-und-wie-funktioniert-webtracking/23386>. Accessed 4 Apr 2017
- Schleipfer S (2015) Datenschutzkonformer Umgang mit Nutzungsprofilen. ZD 5(9):399–405
- Schonschek O (2014) App-Tracking: Was Apps alles verraten. Datenschutz-Praxis.de. <https://www.datenschutz-praxis.de/fachartikel/app-tracking-apps-alles-verraten/>. Accessed 4 Apr 2017
- Schultski-Haddouti C (2015) Ein bisschen Datenschutz ist schon eingebaut. FAZ.net. <http://www.faz.net/aktuell/technik-motor/computer-internet/privatsphaere-und-tracking-ein-bisschen-datenschutz-ist-schon-eingebaut-13838753.html>. Accessed 4 Apr 2017
- Sueddeutsche.de (2015) Datenschützer: Facebook hat keinen Respekt vor Privatsphäre. <http://www.sueddeutsche.de/digital/tracking-datenschuetzer-facebook-hat-keinen-respekt-vor-privatsphaere-1.2483240>. Accessed 4 Apr 2017
- Sueddeutsche.de (2016) Französische Datenschützer werfen Facebook Gesetzesverstöße vor. <http://www.sueddeutsche.de/news/service/internet-franzoesische-datenschuetzer-werfen-facebook-gesetzesverstoesse-vor-dpa.urn-newsml-dpa-com-20090101-160209-99-585875>. Accessed 4 Apr 2017
- Unabhängiges Landeszentrum für Datenschutz (2011) Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook. <https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf>. Accessed 4 Apr 2017

Author Biography

Charlotte Röttgen Ass. iur., research associate at the Institute for Information, Telecommunication and Media Law (ITM) at the University of Münster. She studied law in Bielefeld, Santiago de Compostela and Münster, from where she holds a law degree. Charlotte completed his legal clerkship at the District Court of Münster.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

