THE LEGAL®EVOLUTIONARY

Web Tracking meets Data Privacy (Part 2)

German Telemedia Act and GDPR

Dr. Jörg Kaufmann, Lawyer, Schadbach Rechtsanwälte

9. September 2019

LR 2019, Seiten 113 bis 122 (insgesamt 10 Seiten)

Part 1 of this essay examines the technical background of web tracking as a means of collecting information for the purposes of marketing.[1] Part 2 deals with the data privacy implications of web tracking.[2] 1

I. Data Privacy Law

1. The Nexus between Web Tracking and Data Privacy

Web tracking involves the processing of large amounts of data. This raises the question as to whether data privacy law puts restrictions on web tracking. According to art. 1 para. 1 of the European General Data Protection Regulation (GDPR), the regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data, as well as rules relating to the free movement of personal data. 2

a. Definition of Personal Data

Art. 4 no. 1 GDPR offers a definition of the term 'personal data' by explaining it as any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. It can be inferred from this definition that an online identifier may qualify as personal data, even though no specific criteria for handling the question of identifiability are provided. 3

[1] Kaufmann, Web Tracking meets Data Privacy (Part 1), LR 2019, 88, https://www.legal-revolution.com/de/the-legal-revolutionary/itk/web-tracking-meets-data-privacy-part-1.

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

b. Online Identifiers as Personal Data

Recital 30 GDPR states that natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them. According to recital 26 GDPR, in order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the cost of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. 4

Recital 26 GDPR states that the answer to the question of identifiability depends on the effort that is required to identify the natural person.[3] In contrast, recital 30 GDPR suggests that any identifier, including an online identifier, relates to an identifiable natural person.[4] Recital 30 GDPR is in line with the fact that data from different processing activities can easily be combined into a set of information that allows the identification of a natural person. There is hardly any data left that cannot be related to an identifiable natural person.[5] The straightforwardness of the approach taken in recital 30 GDPR will ensure its widespread adoption. In all likelihood, data protection authorities will be of the opinion that identifiers such as IP-addresses or web cookies are personal data according to art. 4 no. 1 GDPR.[6] Online advertisers are advised to take this fact into account when implementing advertising measures.[7] 5

2. Pre-GDPR Legal Situation

a. ePrivacy Directive and Cookie Directive

European lawmakers have always handled the question of data privacy in the telecommunications sector as a specific issue that requires regulation outside of the general data privacy regime.[8] The precursor of the General Data Protection Regulation 6

[3] *Härting*, DSGVO, 2016, rec. 281.
[4] *Härting*, DSGVO, 2016, rec. 279.
[5] *Veil*, NVwZ 2018, 686, 693.
[6] *Härting*, DSGVO, 2016, rec. 280.
[7] *Schirmbacher*, ITRB 2016, 274, 275.
[8] *Härting/Gössling*, CRi 2018, 6.

(GDPR)[9] was the European Data Protection Directive 95/46/EC.[10] This Directive was complemented and particularised by the ePrivacy Directive 2002/58/EC.[11] The latter deals with the processing of personal data and the protection of privacy in the electronic communications sector.[12]

The Cookie Directive 2009/136/EC has led to changes in Art. 5 para. 3 ePrivacy Directive on the use of information on terminal equipment, especially with regard to cookies. Art. 5 para. 3 ePrivacy Directive requires the user's informed consent to the storing of information, or the gaining of access to information already stored in the terminal equipment of a user. The user's consent is not required, however, if a) the cookie is used for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or b) the cookie is strictly necessary in order for the provider of an information society service explicitly requested by the user to provide the service. Art. 5 para. 3 ePrivacy Directive is applicable whether or not the information in question qualifies as personal data.[13] 7

The ePrivacy Directive 2002/58/EC granted the user only a right to refuse (opt-out) to the storing of or gaining access to information on his/her terminal equipment. The changes in art. 5 para 3 ePrivacy Directive by the 2009 Cookie Directive demonstrate that the disagreement over the consent requirement (opt-in) as opposed to an opt-out right of the Internet user already started several years ago. Moreover, the complicated wording of art. 5 para 3 ePrivacy Directive highlights a basic problem pertaining to data privacy law. In this field of the law, we frequently encounter approaches that are not suitable for handling complicated technical matters. From a practical point of view, the exceptions to the consent requirement in art. 5 para 3 ePrivacy Directive are difficult to handle. In order to determine whether a cookie is "strictly necessary" for the provision of an information society service, a profound understanding of the technical properties of the cookie is required. 8

b. Sec. 15 para. 3 German Telemedia Act

In Germany, the Data Protection Directive 95/46/EC was implemented mainly by the Federal Data Protection Act (BDSG). However, according to sec. 1 para. 3 BDSG more specific federal data protection provisions took precedence over the BDSG regulations. The German Telemedia Act (TMG) contains specific provisions in the sense of sec. 1 para. 9

[9] According to Art. 288 para. 2 TFEU a regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States.
[10] According to Art. 288 para. 3 Treaty on the Functioning of the European Union (TFEU) a directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.
[11] Art. 1 para. 2 ePrivacy Directive.
[12] See art. 1 para. 1 ePrivacy Directive.
[13] *Hanloser*, ZD 2018, 213, 214; *Schwartmann/Benedikt/Jacquemain*, PinG 2018, 150, 152.

3 BDSG on the processing of personal data with regard to electronic information- and communication services that are not telecommunication services or radio broadcasting.[14]

According to sec. 15 para. 3 TMG the provider of telemedia services may – for the purposes of advertising, market research or adequate implementation of telemedia services – create user profiles by using pseudonyms, as long as the user does not object. The service provider is under an obligation to inform the user about his/her right of objection in accordance with sec. 13 para. 1 TMG. The user profile must not be combined with data about the person behind the pseudonym. 10

Sec. 15 para. 3 TMG does not deal with technical details such as IP-addresses, web cookies or browser fingerprints. Rather it deals with data privacy regulation on user profiles.[15] The opt-out requirement offers an incentive for trackers to stay within the limits of pseudonymous profiling. The German online advertising industry has always been in favour of the provision in sec. 15 para. 3 TMG[16] because there is no need to collect the user's consent. 11

There is a contradiction between art. 5 para. 3 ePrivacy Directive and sec. 15 para. 3 TMG.[17] Art. 5 para. 3 ePrivacy Directive requires the informed consent of the user to the storing or accessing of information on his/her terminal equipment. In contrast, sec. 15 para. 3 TMG allows pseudonymous profiling under the condition of the user's opt-out right. The German federal government was of the opinion that art. 5 para. 3 ePrivacy Directive had been fully implemented into German law.[18] However, the argumentation of the German government did not take sec. 15 para. 3 TMG into account. This statutory provision does not require the user's consent to the creation of pseudonymous user profiles.[19] The German data protection authorities declared that the German Telemedia Act was an insufficient implementation of art. 5 para. 3 ePrivacy Directive, because the consent requirement had not been implemented into German law.[20] In any case, German Internet users could not claim direct applicability of the Cookie Directive vis-à-vis private 12

[14] Sec. 1 para. 1 TMG.
[15] *Schleipfer*, ZD 2017, 460, 461.
[16] *Schürmann*, DSB 2017, 9, 11.
[17] *Bauer* et al., BVDW-Whitepaper, Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte, 2015, 11, https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/data_economy/whitepaper_targeting_browsercookies-und-alternative-trackingtechnologien_2015.pdf.
[18] *EU-Commission*, Questionnaire on the implementation of Article 5 (3) ePrivacy Directive, COCOM11-20, with answers from the German Federal Government, https://www.telemedicus.info/uploads/Dokumente/COCOM11-20QuestionnaireonArt.53e-PrivacyDir.pdf.
[19] *Jandt*, ZD 2018, 405, 407.
[20] Umlaufentschließung der Datenschutzbeauftragten des Bundes und der Länder, February 5, 2015, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2015/2015-DSK-Cookies.pdf.

telemedia providers.[21] Therefore, the service providers only needed to fulfil the requirements of sec. 15 para. 3 TMG in relation to pseudonymous user profiling.

c. Usefulness of the Consent Requirement

The ongoing discussion about the consent requirement raises the question of the usefulness of the consent declaration that is provided online by the data subject. Only very few Internet users read a privacy policy when being asked to consent to it. In the face of heightened GDPR awareness, attentive readers may choose to reject a privacy policy. This usually means that as a result they are denied access to certain services in which they were originally interested. The act of saying no is therefore considered an act of self-determination. In the vast majority of cases, however, Internet users simply give their consent by ticking a box on a formulated declaration.[22] Privacy policies are highly standardised, which means that Internet users are confronted with a take-it-or-leave-it situation.[23] More often than not, consent declarations and the privacy policies to which they refer are incomplete, inaccurate, and misleading. There can be no reasonable expectation of users reading or understanding privacy policies. In addition, being confronted with a banner containing a consent declaration is, for many users, as irritating as advertising banners. As a result, many users click the consent box as a means of clearing away the privacy banner, which in this case is received as screen pollution. The extent to which the mouse click over the putative consent declaration box can therefore be considered actual consent is therefore questionable.[24] 13

Website operators, trackers and online advertisers (data controllers) are not necessarily in favour of having to collect consent declarations either. The user may revoke his/her consent at any time[25] and the data controllers need to be able to prove that the consent declaration was actually given.[26] The wording of the consent declaration may force data controllers to directly confront the Internet user with certain information which they would rather bury in long-winded privacy policies. Moreover, there is always a chance that a consent declaration proves invalid. This leaves data controllers open to the risk of being fined by data protection authorities. A consent requirement therefore serves neither Internet users, website operators, trackers nor online advertisers. 14

The practical uselessness of a consent declaration does not affect its legal value as a ground for the lawfulness of processing according to art. 6 para. 1 lit a) GDPR. Yet why are so many data privacy stakeholders in favour of the consent as the most suitable ground 15

[21] *Lotze/Heinson/Hasselblatt*, MAH Gewerblicher Rechtsschutz, 5th edition 2017, sec. 30, rec. 106.
[22] *Härting*, Internetrecht, 6th edition 2017, Datenschutzrecht, rec. 216.
[23] *Veil*, NVwZ 2018, 686, 688.
[24] *Härting*, CR 2014, 528, 533.
[25] Art. 7 para. 3 GDPR.
[26] Art. 7 para. 1 GDPR.

for the lawfulness of processing? For example, German data protection authorities champion the consent requirement in the web tracking scenario.[27] According to art. 8 no. 1 lit (b) draft ePrivacy Regulation,[28] the end-user's consent is a legitimate ground for the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including information about its software and hardware. One possible answer might be that we simply want to maintain the "delusion that consent can sanitize questionable privacy practices."[29] Or another answer might lie within the pressures that are exerted on the developers of web tracking technologies to be consistently innovative and competitive. In this case, data privacy law consistently lags behind new developments in web tracking procedures. The very notion of user's consent presupposes informational self-determination, thus making it attractive to data protection authorities and lawmakers because the responsibility for that consent can be shifted onto the data subject.

3. Post-GDPR Legal Situation

a. GDPR and German Telemedia Act

The GDPR has been applicable since 25 May 2018. According to recital 173 GDPR, the regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective as set out in the ePrivacy Directive 2002/58/EC, including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between the GDPR and the ePrivacy Directive, the ePrivacy Directive should therefore be amended in order to ensure consistency with the GDPR. 16

The ePrivacy Regulation, the successor of the ePrivacy Directive, was supposed to become applicable on the same day as the GDPR.[30] Yet the ePrivacy Regulation is still under discussion and will probably not be applicable before 2022. Until the ePrivacy Directive is amended by the ePrivacy Regulation, the relationship between the GDPR and the ePrivacy Directive is governed by art. 95 GDPR.[31] According to art. 95 GDPR, the regulation shall not impose additional obligations on natural or legal persons in relation to processing in 17

[27] Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, April 26, 2018, 3, rec. 9, https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf.

[28] Discussion Paper (6771/19) regarding the ePrivacy Regulation, February 4, 2019, https://www.bvdw.org/fileadmin/bvdw/upload/dokumente/recht/e_privacy_verordnung/20190225__Ratsdokument_ePrivacy_vom_22._Februar_2019.pdf.

[29] *Peppet*, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, Texas Law Review 2014, 85, 159, https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf; *Härting*, CR 2014, 528, 533.

[30] *Rauer/Ettig*, ZD 2018, 255.

[31] *Schwartmann/Benedikt/Jacquemain*, PinG 2018, 150, 151.

connection with the provision of publicly available electronic communications services in public communications networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in the ePrivacy Directive 2002/58/EC.

Even though the GDPR has been applicable since 25 May 2018, German lawmakers have not adapted sec. 13 et seq. of the Telemedia Act. This remarkable oversight has led to a questioning of the relationship between the GDPR and the data privacy regulations in the German Telemedia Act.[32] The ePrivacy Directive and sec. 13 et seq. of the German Telemedia Act do not in fact have the same scope. Websites, apps and other Internet based services are not publicly available electronic communications services in public communication networks. Rather they are information society services according to art. 1 no. 2 Directive 98/34/EC in conjunction with art. 2 lit a) Directive 2000/31/EC.[33] The data privacy provisions in the German Telemedia Act are primarily an implementation of the Data Privacy Directive 95/46/EC. The application of these data privacy provisions cannot be based on Art. 95 GDPR.[34] Neither can the application of sec. 13 et seq. TMG be based on any opening clauses in the GDPR that allow for specific national data protection regulation.[35] The data privacy provisions in the German Telemedia Act are therefore no longer applicable.[36] 18

b. GDPR and Web Tracking

As long as the ePrivacy Regulation has not entered into applicability, the online processing of personal data is governed only by the GDPR.[37] Unlike the German Telemedia Act, the GDPR does not contain any specific provisions on user profiles with regard to telemedia services.[38] According to recital 72 GDPR, profiling is subject to the rules of the GDPR governing the processing of personal data, such as the legal grounds for processing or data protection principles. The lawfulness of all data processing with regard to web tracking is therefore subject to art. 6 para. 1 GDPR.[39] There is no ranking between the 19

[32] *Jandt*, ZD 2018, 405, 406; *Sesing,* MMR 2019, 347.
[33] *Schwartmann/Benedikt/Jacquemain*, PinG 2018, 150, 152.
[34] *Sesing*, MMR 2019, 347, 349.
[35] *Jandt*, ZD 2018, 405, 407.
[36] *Härting*, Internetrecht, 6th edition 2017, Datenschutzrecht, rec. 222; *Forgo/Helfrich/Schneider/Bierekoven*, Betrieblicher Datenschutz, 3rd edition 2019, rec. 86; *Plath*, DSGVO/BDSG, 3rd edition 2018, rec. 2; Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, April 26, 2018, 2, https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf.
[37] *Jandt*, ZD 2018, 405, 407.
[38] *Härting*, Internetrecht, 6th edition 2017, Datenschutzrecht, rec. 222.
[39] *Forgo/Helfrich/Schneider/Bierekoven*, Betrieblicher Datenschutz, 3rd edition 2019, rec. 88; *Schirmbacher*, ITRB 2016, 274; *Schwartmann/Benedikt/Jacquemain*, PinG 2018, 150, 152; *DSK Datenschutzkonferenz*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, March 2019, 7, https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.

different grounds for the lawfulness of data processing.[40] Therefore, the lawful use of tracking methods does not necessarily require user's consent according to art. 6 para. 1 lit a) GDPR.[41]

aa. Art. 6 para. 1 lit f) GDPR – Legitimate Interests

According to art. 6 para. 1 lit f) GDPR, the processing of personal data is lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. According to recital 47 S.1 GDPR, determining the legitimate interests of the controller has to take the "reasonable expectations" of the data subject into account. To this extent, the awareness by most Internet users of the fact that online services use web tracking devices is of critical importance. The reasonable expectations of the Internet user can therefore be used to justify web tracking procedures, as long as they stay within certain limits. 20

We may question, however, whether Internet users expect being tracked by third parties[42] or even across devices.[43] It is undoubtedly the case that third-party and cross-device web tracking are very common these days.[44] German data protection authorities are critical, however, of justifying these forms of web tracking with art. 6 para. 1 lit f) GDPR.[45] In practice, website operators, trackers and online advertisers cannot be certain of the lawfulness of third-party and cross-device tracking unless they consult directly with the data protection authorities. Ultimately, the "reasonable expectations" of the Internet user will be determined by the data protection authorities. 21

bb. Art. 6 para. 1 lit a) GDPR – Consent

According to art. 6 para. 1 lit a) GDPR, the processing of personal data is lawful if the data subject has given consent to the processing of his/her personal data for one or more specific purposes. The requirements of the consent are governed by art. 4 no. 11, 6 lit a), 7 and 8 GDPR.[46] The user's consent must be granted before the beginning of the processing of personal data. According to art. 7 para. 1 GDPR, proof is required that the user has given his/her consent. In addition, art. 7 para. 3 GDPR stipulates that the data subject shall have the right to withdraw his/her consent at any time. 22

[40] *Schirmbacher*, ITRB 2016, 274.
[41] *Gierschmann*, ZD 2018, 297, 300.
[42] *Schwartmann/Benedikt/Jacquemain*, PinG 2018, 150, 154.
[43] *Schirmbacher*, ITRB 2016, 274, 278.
[44] *Jandt*, ZD 2018, 405, 408.
[45] *DSK Datenschutzkonferenz*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, March 2019, 11 et. seq., https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.
[46] *Schwartmann/Benedikt/Jacquemain*, PinG 2018, 150, 155.

According to art. 4 no. 11 GDPR, "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. According to recital 32 GDPR this may include ticking a box when visiting an Internet website, choosing technical settings for information society services or another statement or conduct that clearly indicates in this context the data subject's acceptance of the proposed processing of his/her personal data. Silence, pre-ticked boxes or inactivity are not an appropriate basis for consent. Opt-out procedures cannot therefore serve as a basis for valid consent according to art. 4 no. 11 GDPR. 23

The consent of the user may be collected with the opening of a user account.[47] The use of cookie banners may also be an appropriate procedure to collect the consent.[48] However, cookie banners that contain only an OK-button are insufficient because these buttons do not offer the opportunity to the Internet user to object to the setting of cookies. Moreover, cookie banners must not block access to a website's imprint and data privacy policy. 24

cc. Provision of Information

Data controllers such as website operators are under an obligation to provide Internet users with certain information about the processing of personal data, especially in accordance with sec. 13 GDPR. However, website operators are usually not fully informed about the data processing by third parties such as advertising networks.[49] In this case, website operators will be unable to fulfil the requirements of art. 13 GDPR. 25

II. Conclusion

There has been a long disagreement over the lawfulness of the processing of personal data with regard to web tracking. Central to the debate has been the dispute over the consent requirement (opt-in) as opposed to a right of objection of the Internet user (opt-out). Given the practical uselessness of a consent declaration, however, the debate is pointless. There is a fundamental misfit between the tools of data privacy law and the complexities of web tracking. Yet public stakeholders, such as data protection authorities, are nevertheless in favour of the consent requirement. In all likelihood, the dispute over this requirement will continue into the foreseeable future. 26

Web tracking and data privacy law are in their current formulations difficult to reconcile. Third-party and cross-device web tracking are the pillars of the online advertising industry, 27

[47] *Schirmbacher*, ITRB 2016, 274, 278.
[48] *DSK Datenschutzkonferenz*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, March 2019, 9, https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.
[49] *Schwartmann/Benedikt/Jacquemain*, PinG 2018, 150, 154.

and yet data protection authorities are critical of these forms of web tracking. Collecting users' consent does not help the problem of the data controller, who is required to provide the Internet user with certain information, especially according to art. 13 GDPR. Website operators, trackers and online advertisers are, as a result, consistently confronted with a situation of legal uncertainty.