Research Article

Timo Jakobi*, Gunnar Stevens, Anna-Magdalena Seufert, Max Becker, and Max von Grafenstein

Web Tracking Under the New Data Protection Law: Design Potentials at the Intersection of Jurisprudence and HCI

<https://doi.org/10.1515/icom-2020-0004>

Abstract: The GDPR regulates at present the handling with personal data fundamentally new and thereby opens new leeway. At the same time, it creates great uncertainty among those affected. One example of this is web tracking: It helps designers to improve the utility and usability of their websites based on, in part, extensive (personal) data collection, or enable operators to finance them. Against this background, in this article we first show the practical relevance of web tracking by collecting the web trackers of the 100 most popular pages of each of the 28 EU member states. Building on this, we show which data these trackers collect and analyze their legal bases. Finally, we discuss possible consequences in design and architecture for fulfilling the legally outlined requirements, taking into account a user's perspective.

Keywords: Web-Tracking, Privacy, Data protection, GDPR, HCI

1 Introduction

By 2021, more than half of the world's population is expected to be online, using websites for a variety of purposes on a daily basis [31]. To be able to offer content without financial compensation, these are financed to a large extent by advertising revenues [6]. Equally, an important aspect is the analysis of user behaviour to improve one's own service [15], or the integration of social media features such as Facebook, Twitter, and others [50]. In this context,

external service providers are often involved for the provision of advertising, analysis, etc. This constellation has legal implications (concerning collection, processing and transfer of personal data amongst these parties) which in turn may affect the design and the design process. The ongoing legal discussion shows parallels with research in the field of Usable Privacy, where decision support and awareness mechanisms are investigated, e. g. in the context of authorisation of mobile apps [5, 26, 64]. Among other topics, in particular, user-centred design of general terms and conditions as well as privacy policies [4, 14, 73] are being researched, much like the legality, design and user-friendliness of cookie banners [19]. More recently, research has started to embrace tracking technologies [10, 50, 66], too.

One important incentive for these efforts is provided by new legal frameworks, which are emerging globally, such as the General Data Protection Regulation (GDPR) [25], which has been in force since 2018. Moreover, in Europe, with currently postponed e-Privacy Regulation, new legislation specifically targeting web privacy is underway [24]. In this regard, research has especially looking at the use of web tracking after GDPR coming to effect [61]. Similarly, the prevalence of third parties on web sites [70], and more specifically the use of cookies [19] and web tracking [66] has recently come to focus of research on Usable Privacy.

Beyond understanding the spread of such tracking technologies – often used for the sake of online behavioural advertisement –, arguably the new legal landscape also demands research for (potentially: new) legally legitimate design interpretations. While users often have a certain basic sensitivity with regard to the handling of personal data on the Internet [37], information about the use of trackers by the site operators is only rarely provided. If so, the information is difficult or cumbersome to obtain for the average user, leaving a “blind spot” that still has to be legally developed [45]. In this regard, the extent and especially the data collection practices of web tracking have so far undergone less detailed review. These, however, are

***Corresponding author: Timo Jakobi**, University of Siegen, Siegen, Germany, e-mail: timo.jakobi@uni-siegen.de

Gunnar Stevens, Anna-Magdalena Seufert, Max Becker, University of Siegen, Siegen, Germany, e-mails:

gunnar.stevens@uni-siegen.de,

anna-magdalena.seufert@uni-siegen.de,

m.becker@recht.uni-siegen.de

Max von Grafenstein, Einstein Center Digital Future, Berlin, Germany, e-mail: m.von-grafenstein@udk-berlin.de

a key basis for discussing viable solutions for the future of both legal and more user-friendly online tracking. Both from a legal and design perspective, more detailed information on data collection practices are desirable to inform ongoing legislative processes and potential design in this area.

Against this background, this paper reports on an analysis of practices of data collection, processing and obtaining user consent of web tracking services on the most popular websites of the EU-28. In a second step, and in light of the revised and evolving legal situation, the paper discusses requirements from a legal and users' point of view in this multi-stakeholder environment, with conflicting interests between website operators, jurisdiction and users. Finally, we propose how HCI can contribute to an interpretation of the legal situation and the development of usable and effective tools for controlling and informing about trackers.

2 Web Tracking: Technology, User, Legislation

In this section, we first introduce into related research on the topic of web trackers. We focus on the two perspectives of human-computer interaction and jurisprudence.

2.1 Techniques of (Defying) Web Tracking

Web tracking has found wide application [66], whereby by its high market penetration the company Google occupies a special position [43, 60, 66]. Various studies suggest that online tracking is used to personalize online advertising based on sensitive information [18, 28], (to the point of creating detailed personality profiles [79]) discriminate against users [18] or manipulate their buying intentions [13].

With regard to tracking methods, a distinction can be made between “stateful” and “stateless” tracking [50], depending on where the relevant data is stored to enable tracking. Bujlow [10] distinguishes four methods even more finely: Sessions, client memory, client cache and fingerprinting based tracking. In a detailed literature review, Ermakova et al. [23] have shown that although private-friendly methods for web tracking exist [3, 63], they have not yet established themselves.

On the other hand, there are various tracking protection approaches [41, 53, 78], such as detecting tracking code and preventing its execution, blocking access

to known tracking domains, and preventing the outflow of tracking information by analyzing outgoing HTTP requests. There are also a number of browser settings and extensions such as Ghostery, Adblock Plus or Disconnect, which support users to prevent unwanted tracking [53].

It turns out, however, that their effectiveness is limited [53, 56]. In particular, tracking and tracking protection techniques show a kind of arms race between advertisers and the privacy protection community [54]. A field study by Achara et al. [1] shows that the use and control of protection tools can overcome a total blockade and thus also meet economic interests.

2.2 (Involuntarily) Affected Parties of Web Tracking

From the point of view of the user or, to be more precise, the data subject (as the terminology of GDPR defines), surveys indicate that tracking is an interference with privacy and harassment by unwanted advertising. For example, a survey conducted in the US in 2009 showed that 87 % of respondents would reject individualized advertising if they had a choice. [74]. This finding could be confirmed by other studies [51, 58]. However, there is a gap between attitude, intention and actual behaviour [2].

There are several reasons that can explain this gap: On the one hand, user attitudes towards tracking for personal advertising, in particular, are complex, contextual and difficult to understand on close examination. In a qualitative study, Melicher et al. [52], for example, recorded browser histories and, on the basis of this, had them reflected on the users' respective web usage. This revealed varying settings for tracking and the circumstances under which users considered the recording to be legitimate. Similar studies on personalized advertising indicate that acceptance is highly contextual [36, 75]. The Ackerloff effect [7] is even more pronounced among trackers than in the case of consent issues in more transparent data protection issues. Moreover, as Sakamoto et al. [61] show, counter-intuitively, explicitly opting-out of online behavioural advertising leaves companies with room to still track users, even after introduction of GDPR. The information asymmetry between operators of trackers and end-users is so extensive that the market (if one can even speak of a market in this case) fails to function. If 50 or more trackers collect personal data on a homepage and pass it on to an unmanageable number of third parties, this is based on a strongly one-sided and hardly consensus-oriented business model (referred to by Zuboff as “surveillance capitalism” [79]). Another reason for the intention-behaviour gap is the lack

of user acceptance of the existing possibilities to prevent (personalized) advertising [9]. This is due to a lack of usability of the tools for protection. Studies point out that the self-explanatory ability is inadequate so that the tools themselves can cause comprehension problems [57, 65]. Furthermore, existing solutions are often very technically designed, so that they are difficult and time-consuming to implement for the user [45]. In particular, most solutions are not protection by default, so that the user himself must become active in order not to release data. In order to reduce the complexity for the user, Melicher et al. [2] have proposed design guidelines in which (semi-)autonomous agents can take over the tasks of tracking protection. They also propose that tracking protection should be accompanied by appropriate legal intervention.

2.3 Legal Regulation on Web Tracking

Since May 25, 2018, the GDPR has regulated the handling of personal data in a binding manner throughout Europe. Particularly in the online area, there was much discussion in advance about what still would be permitted with the deadline and what would not [69]. In this context, it should be noted that, at no point, legislator intended to prevent any data processing or to destroy entire business purposes through the GDPR. The protective purpose of the GDPR is to enable individuals, against the background of modern data processing possibilities and techniques and their risks, to decide for or against consent to data processing on the basis of appropriate information on how their personal data is handled and in a self-determined manner [44, 72].

Especially questions on data processing in the online area (e. g. on range measurement and the use of tracking tools for online services) are to be regulated in the pending ePrivacy Regulation. However, it remains to be seen how sharply this law will be fleshed out, as it is a) still not foreseeable in its content and b) very much under the influence of various stakeholders. One of the main questions – and a reason for the delay – is a conflict over the conditions for the use of trackers and the protection of the data subject against them (more on this in 2.4 Legal classification). Several drafts suggested that current forms of data processing could, with a few exceptions, be rendered fundamentally inadmissible. In addition to the purpose of providing the service in question, the exceptions would also include the consent of the user.

Originally, the ePrivacy Regulation was supposed to come at the same time as the GDPR. By now, drafts for the Regulation are available by the European Parliament and

the European Commission. However, the final draft by the European Council is still missing. Many drafts were proposed and failed in Council during the past EU Presidencies (latest: Finland, upcoming: Croatia). Since without a final draft of the Council, the trilogue procedure cannot proceed, it is highly unlikely to see the Regulation passed even in 2020. On December 3, 2019, EU-Commissioner for Communications Networks, Content and Technology, Thierry Breton, even mentioned a total realignment of the negotiations [22, 83].

These circumstances beg the question, which laws apply until the ePrivacy Regulation comes into force and how tracking can be designed in conformity with the foreseeable regulations.

2.3.1 Legal Classification

Against this background, this section outlines the legal provisions on tracking in more detail. The Telemedia Act (TMG) in §§ 12, 13, 15 permitted such user profiles that only contained anonymous or pseudonymous data, whereas personal user profiles were only permitted with suitable consent. In addition, there was a ban on merging different user-profiles and users had the right to object to the creation of user profiles. The provider had to inform users about the creation of user-profiles and about their right to object [67]. In principle, it can be argued, that the lack of attention and knowledge about tracking practices has been noticed and addressed by German legislation with the TMG.

The TMG was applicable in Germany until May 25, 2018, and was then superseded by the GDPR [71, 67]. In the future, its area will be governed by the so-called “ePrivacy Regulation”, which is the successor to Directive 2002/58/EC of the European Parliament and of the Council of July 12 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, known as the “ePrivacy Directive”. This directive was revised in 2009 by the so-called “Cookie Directive” (2009/136/EC), which, however, was not implemented in Germany. Instead, the “storage” and “access to information already stored in the terminal device of a subscriber or user” provided for in Art. 5 (3) of the Cookie Directive with the reservation of consent were regarded as covered by § 15 (3) TMG.

Said envisioned regulation, however, is still lacking a draft of the European Council to proceed [24]. According to the draft version, the “use of the processing and storage functions of terminal equipment and any collection of information from terminal equipment of end-users” should

only be permitted with the consent of the user (with a few exceptions such as service provision and for security reasons), Art. 8 (1) ePrivacy Regulation draft. As a result, target group-oriented advertising, range measurement, campaign tracking, payment models etc. would only be possible with the legally binding consent of the user.

Also, according to the draft, the ePrivacy Regulation provides for a blanket declaration of consent through browser settings. This means that browsers “offer the possibility of preventing third parties from storing information in the terminal equipment of an end-user or from processing information already stored in the terminal equipment”, Art. 8 (1) lit. c) in conjunction with Art. 10 (1) (draft version). However, the whole draft and, in particular, the rule cited above are controversial. For example, there was an outcry among press publishers (“publishers are concerned that it will be incredibly difficult to persuade readers to change their browser settings to allow 3rd party cookies”). In response to a parliamentary question, the Federal Government replied that it had submitted an amendment proposal for Art. 8, according to which “online services financed by advertising should have the possibility of making the use of such services dependent on consent to cookies for advertising purposes” [11]. One could also polemically speak of tying permission, i. e. the softening of a strictly private solution.

This shows, by way of example, which conflicts of interest still exist with regard to the ePrivacy Regulation and explains why the legislative process is taking so long. There are three points of contention:

1. The question of the type and scope of permissible processing of metadata without the consent of the end-user concerned for the provider’s commercial purposes;
2. the design of the guidelines on the use of cookies and trackers on terminal devices or access to information available in the terminal device, and finally
3. the scope of application of the ePrivacy Regulation and the relationship as special legislation to the GDPR [11].

The points also indicate why the lowering of the level of data protection is often feared in comparison to times of applicability of the TMG [38, 67].

With the delay and lack of clarity regarding the further course of the ePrivacy Regulation, the question arises as to which provisions are applicable in the meantime. The “Position Paper of the Data Protection Conference” (released April 26th, 2018) [8, 40] addresses this question, although fairly debated and criticised. Accordingly, Art. 6 (1) lit. a), b) and f) of the GDPR will apply from May 25, 2018 on.

While the option under lit. a) relies on the legitimate consent of the data subject, processing operations that are absolutely necessary for the provision of the service requested by the data subjects can be based on lit. b). In this vein, the balancing of the interests of the person responsible and the data subject under lit. f) is particularly interesting, as it is a possibility that goes beyond the planned options of the ePrivacy Regulation.

The decisive factor here is that a legitimate interest of the person responsible (e. g. to secure the systems; but also for marketing purposes, e. g. for personalised advertising, if certain protective measures have been taken) can be affirmed (Recital 47 in: [25]). This must be weighed against the interests of the data subject worthy of protection, taking into account the circumstances of the individual case (e. g. protection against inappropriate monitoring of online activities and profiling; as well as further interests or fundamental rights and freedoms of the data subject [77]).

At this point, it additionally has to be stressed that the European Court of Justice lately judged the legitimacy of cookies and clarified that cookies under the GDPR are only legal with the user’s permission [80].

2.3.2 Takeaways from the Ongoing Cookie Debate

Especially since introduction of GDPR, there have been some major developments in handling of third-party cookies, both in legislation and case law as well as in the practical application. For example, studies have shown how both the use of third-party cookies and the information of users as well as the design of interfaces to opt-out of cookies have changed quite dramatically [19, 70].

During the past months there have been two important judgements by the ECJ concerning Tracking-Cookies and the necessity of (informed) consent in data processing:

The first judgement, based on a case originally from 2015, was spoken in July 2019. The consumer centre of North Rhine Westphalia filed an injunction against Fashion ID, an online retailer, who used the Facebook-Plugin on its website. The consumer protectors rated this as a violation of the GDPR since, even if the user owns no Facebook profile at all, the site operator would pass the users data (as e. g. IP address and web browser-ID) to Facebook, simply by integrating the application in their website. Based on that, the consumer centre requested users should have been informed about the tracking procedure and warned the company. The lower court agreed with the consumer centre and confirmed that the site operator is responsible for the violation of data protection law.

The Higher Regional Court of Düsseldorf asked the ECJ to answer the basic questions concerning the legal situation in terms of data protection law in this case. The ECJ decided that an informed, demonstrable and revocable declaration of consent by the user before the tracking starts is mandatory [81]. (This means, a cookie banner in the form most commonly used is not adequate.) It does not bother if Cookies store personal or anonymous data. Only so-called “first party cookies” are not included. Furthermore, each website operator is jointly responsible (together with Facebook) for the Plugin and the resulting data processing. But there is a restriction: Website operators are not liable for the whole process of creating a profile through Facebook. The joint responsibility is limited to the process of data transmission, because the operator decides “about the purposes and means” of the processing. In this, it does not matter that website operator do not have any influence on the data transmission by the application. Since they benefit from it, e. g. from higher range, they are jointly responsible. Finally, it has to be said that most buttons, tools and plug-ins (mostly from services based in the US, e. g. like Twitter, Instagram, LinkedIn, to name a few) are working in the same scheme (which means, they transmit user data without permission). Therefore, the judgement applies correspondingly.

The second judgement, known as “Planet49” [80] was spoken at October 1st, 2019. The original case was a suit between “Planet 49 GmbH” and the German National Association of Consumer Centres. In 2013, Planet 49 offered participation at a winning game on a website. During the process, the user was asked for its permission in setting cookies on the computer used and thus making it possible to evaluate surfing and usage behaviour for advertising purposes. In this case, the declaration of consent was based on a pre-checked box, with the consequence that users had to opt-out in case of disagreement. The German National Association of Consumer Centres valued this design as an infringement against data protection law and requested omission. The Federal Supreme Court asked the ECJ for Interpretation of the relevant Union law regulations.

Again, the ECJ judged [82]:

- If a consent is mandatory, the user has to issue it expressly. An opt-out solution is not sufficient.
- A consent needs to be informed to be lawfully. This means the website operator has to give information about functionality of the Cookies, storage duration and third-party access.
- The European regulations on the protection of privacy in electronic communication are applicable no matter, if those data are personal or not. European law should

grant protection against intrusion into privacy, among others against unauthorized entry into the users’ devices.

It has to be said that the ECJ transferred both cases back to the German courts to finally decide on. However, the assessments of the ECJ must already be taken into account when applying data protection law (and German regulatory authorities have been confirmed in their positions and approach).

To sum up: Even if it is disputed how exactly these conclusions must be applied in these and, even more so, other cases, both judgements principally state that consent in data collection and tracking via cookies (any, except first party cookies) is mandatory. It has to be a voluntary, informed, demonstrable and revocable declaration of consent by the user in advance of tracking. It does not bother if the Cookies store personal or anonymous data.

3 Method: Data Corpus and Analysis

This section outlines the methodological details for obtaining the data basis for carrying out the following discussion from a legal and users’ point of view.

The Alexa Top Sites¹ of February 2019 served as the starting point for identifying the 100 most popular pages of each of the 28 states of the European Union. For identifying unique URLs, different country codes of top-level domains were distinguished, resulting in 1,391 websites to be examined for use of web tracking. The Firefox browser plugin lightbeam² was used to count the amount of trackers on each of these websites. For analyzing the trackers for their data collection practices, the study is limited to the ten most common trackers identified in the sample. For this task, the Firefox plugin Ghostery³ was used to search for information provided on data collection and processing practices, including

- the data collected,
- their retention periods,
- the disclosure of this data to third parties, and
- the indication of data processing purposes and
- the specification of a data protection officer or a contact person.

¹ <https://www.alexa.com>

² <https://addons.mozilla.org/en-US/firefox/addon/lightbeam/>

³ <https://www.ghostery.com/>

Data were collected on a computer of the university with the operating system Windows 10 Professional Build 1809 and the Firefox Browser v65.0.2.

These data form the thematic and motivational background for the legal classification of web tracking and discussion of design requirements from a users' perspective. In addition to consulting the various legal provisions, publications (commentary and journal literature) addressing the future ePrivacy Regulation on the requirements for data processing and lawful consent under the GDPR was included in the work on this article.

Figure 1: Amount of trackers found on websites.

4 Findings

This section introduces into the basic quantitative findings and outlines challenges in and ways of accessing tracking information from a user's perspective.

Secondly, data collection and processing practices are outlined for trackers on the most visited European websites. This description serves as a basis for our legal assessment and the discussion of a legally compliant design and use of trackers according to GDPR.

Figure 2: The most popular trackers identified.

4.1 Analysis of Web Tracking

To obtain a more detailed picture of web tracking, it is especially important to consider content a website includes from third party origins. The 1,391 web pages included into the sample, load 33,292 URLs differing from the top-level domain ($\emptyset$: 22.9 URL/page). Filtering calls to each websites' subdomains, 31,063 URLs remain ($\emptyset$: 22.3 URL/page). Regarding the use of trackers on websites, a Poisson distribution approximately fits (Figure 1). 162 pages did entirely without trackers, while a page with 182 trackers occupied the peak value.

A closer analysis of the foreign URLs shows that only 1,871 different top-level domains account for all of these calls. Additionally, different trackers and domains belonging to the same company or group increase this concentration. Domains such as googleapis.com, gstatic.com, googlesyndication.com, googletagmanager.com, googletagservices.com, googleadservices.com, youtube.com and doubleclick.com all belong to the parent company Alphabet. A complete summary of these ties is not provided in this paper, because the organizational or entrepreneurial links between different trackers can hardly be traced in detail. Only for the overview of the top 10 trackers was an attempt made to identify related companies.

The most widespread trackers were clearly assigned to Google, of which accounting for 7,484 hits, making it responsible for almost a quarter of all trackers. Trackers from facebook follow a long way behind, which in turn have a large lead over more specialized companies such as hotjar (visitor behavior analysis), AppNexus, Criteo or Adform (all: sales of personalized advertising).

The ten most widely used trackers of this study (Figure 2) serve as a small sample for a more detailed analysis of the data collection and processing (Figure 3). The information was obtained from Ghostery's information pages to report the data collected.

Interestingly, a fairly well-defined corpus of data collected by the trackers quickly emerged. Although there are some deviations, it becomes clear that many trackers operate on a very similar set of data. Almost all services store the IP address and the device identification number. The collection of browser information, location, and cookies was also very widespread. But even after this top field, the collection is quite homogeneous, especially for anonymous data. When collecting personal data, it is particu-

Figure 3: Information from Ghostery on data collection practices of the ten most common trackers.

larly noticeable that, in addition to address data, payment data is sometimes even processed.

With regard to the further handling of the data, the providers grant themselves quite far reaching rights: The majority of services not only sends aggregated or anonymous data to third parties but also what is considered personal information. Moreover, even with the most widespread trackers, it was sometimes impossible to obtain *any* information regarding the transfer of data to third parties. A similar picture emerged looking at the trackers' specification of the retention period: seven of the ten trackers did not provide any information at all. However, at least they provided the contact details of a data protection officer or a responsible office in the company.

4.2 Assessing the Findings from a Legal Point of View

Due to the uncertainty regarding the ePrivacy-Regulation explained above, the following assessment is based on the GDPR only. This results in a classification of trackers into the categories 'required', 'authorised' and 'consented' and a list of the related legal requirements. The discussion will focus on the requirements of user consent into tracking. However, regardless of the legal basis, beyond consent mechanisms, users must at least be informed about the collection of their personal or personally identifiable information.

A legal definition of consent exists in Art. 4 No.11 GDPR; according to this, consent must be '*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.*'

Informing data subjects (i. e. users whose data are collected) is a central condition and is closely related to the information obligations under Art. 13 (and 14) GDPR. This definition already mentions several of the conditions for consent; furthermore, the conditions in Art. 7 GDPR must be taken into account. Accordingly, there is, among other things, an obligation on the data processor to provide evidence of a data subjects' consent and to inform the data subject of the right to revoke consent at any time with an effect for the future. In addition, the so-called prohibition of coupling in Art. 7 (4) GDPR must be taken into account, according to which it must be examined whether the fulfilment of the contract was made dependent on the consent to the processing of such personal data which is not necessary for the fulfilment of the contract.

A comprehensive duty to inform results from Art. 13 GDPR. Accordingly, the data subject must be informed about e. g.: the responsible entity (including contact data); its data protection officer (if any); the purposes for which the personal data are processed; the legal basis for the processing (including justification and the consequences of refusal e. g. for a conclusion of a contract or the use of a

service). In addition, as far as such a transfer of data happens, information must be provided about the receivers of the personal data and the non-EU states, which data are transferred to.

Finally, users have to be fully informed of their rights. In the case of direct data collection, the information must be provided beforehand. Only in case that data is not raised directly at the data subject, this information has not to be served immediately, but within an appropriate period (at least, within one month); see Art. 14 GDPR. However, it is precisely this information of data subjects, which constitutes a problem: Often, data collection on websites does not only start before a possibly necessary consent could be given, but already before knowledge could be attained at all. Thus, the information duties are not fulfilled in these cases [42]. Finally, it is necessary that the information is specific and, above all, also understandable for the concerning data subjects (both with the obligation to inform according to Art. 13 and Art. 14 GDPR).

Furthermore, in all cases also the general principles from Art. 5 (1) GDPR as well as further relevant defaults, as e.g. Art. 25 (2) GDPR, are to be kept. In relation to the information made available by Ghostery, the following subchapters introduce the information to be determined.

4.2.1 Processing Purposes

A basic obligation in the collection of personal data is the indication of processing purposes for the data collection on the part of the data controller. It is noticeable that either Ghostery does not list these purposes, or (very well possible) that there is no indication of the purpose specification.

4.2.2 Collected Data

As already pointed out, also anonymous or pseudonymous data are collected by the usual trackers indeed, which are not at all or only limitedly covered by the GDPR (see recitals 26 ff to the GDPR). Beyond that, however, almost all trackers also collected personal data in the analysis. In addition, it is to be considered that also anonymous data may become person-relatable by merging with personal data if there is no strict technical-organizational separation of the data (example: Person-relatability of the IP address; judgement of the ECJ: v. 19.10.2016, Az. C-582/14).

4.2.3 Sharing with Third Parties

Practiced by the majority of the services, the transfer of data to third parties is also carried out without information, let alone the naming of a legal basis and information about the purpose or identity of the third party. All of which are basic requirements for the transfer of personal data (which, in principle, can be permitted, for example, on the basis of a contract between a controller and its processor according to Art. 28 GDPR or the transfer to third countries according to Art. 40 ff. of the German Data Protection Act).

4.2.4 Data Retention and Deletion

Regarding the indication of storage duration and deletion periods, it should be noted that on the one hand they can be derived from the purpose, but on the other hand they can also be influenced by statutory provisions (e.g. tax law). Nevertheless, these must be stated, at least if they can be determined.

4.2.5 Information on Rights

It is also particularly (negatively) noticeable that no information, e.g. on rights of withdrawal from profiling, is provided. However, precisely this information about the rights of the data subject is also an important component of either informed (and thus legally binding) consent or legally compliant information in the sense of Art. 13 (and 14) GDPR.

The points mentioned here are to be seen only as examples of (ignored) information duties – as already addressed, these are on the one hand so extensive and on the other hand also individual case-related that a more concrete listing cannot take place here.

5 Discussion

A first challenge for implementations of tracking from a user, technical and legal perspective concerns the effective implementation of a choice to allow or block tracking. While the technical implementation of the actual choice is not very challenging, the legal and design level are more complex. Here, two levels in particular prove to be critical from both a user and a legal perspective: The freedom of choice and the information of the user.

Parallel to the evolving technological developments of tracking (see 2.1) and the complex requirements for user acceptance of tracking (see 2.2), the legal framework, in particular, is currently undergoing major changes, leaving essential leeway for its application in a specific case and thus opening up a design space for (new) interpretations of lawful data collection and processing. In this regard, the present study makes two contributions:

1. In line with existing studies (also on related issues such as third party presence [70] and cookies [19]), it shows that trackers are still widely used even after the introduction of GDPR – raising the question of the legal basis of data processing (Art. 6) and how to ensure lawful use of tracking.
2. Personal data are collected by trackers most often without informing the user. Informing users, however, is necessary as per the principles of art. 5 GDPR – regardless of the justification of the collection.

Subsequently, the discussion will focus on both of these aspects and its implications for design.

5.1 General Legal Options for Lawful Processing of Personal Data in Web Tracking

In general, of the six existing possible justifications according to Art. 6 section 1 GDPR, only the following three can meaningfully be applied to the context web tracking.: contract fulfilment, legitimate interest and users consent.

On a closer look, however, the possibilities are further reduced: First, the basic conditions for a reference to the necessity for the contract fulfilment (lit. b) are quite narrowly put. In addition, it is not to be assumed as a rule that a contract will be concluded solely by calling up a website. Second, the invocation of the legitimate interest (lit. f) presupposes a comprehensive weighing of interests and entails obligations on the responsible party to provide evidence of having conducted such a weighing of interests. Thus, this basis of justification would be associated with a great deal of effort case-by-case. In addition, it also involves a certain legal uncertainty due to the vulnerability of the weighing carried out.

Third and finally, the users' consent (lit. a) arguably constitutes the strongest legal basis for the website provider. It is based on an informed and responsible user who actively communicates a decision regarding the permission of the processing of personal data by trackers. Accordingly, it is attractive for organisations to be able to rely on the informed consent of data subjects because of the

fairly high level of legal certainty. Previous experiences in the context of the introduction of the GDPR show that enterprises frequently rely on such consent mechanisms preventively [16, 55].

Against the backdrop of the three potential justifications for data collection and processing, the following discussion presents different approaches, which are present both in the jurisprudential discourse, HCI research, and practical application [19]:

- **“Cookie Banner 2.0”**: To inform users about the use of tracking mechanisms, information can be displayed by entering a page in the same way as widely used cookie banners. This solution has already been adopted by some organizations, by simply adding information on tracking use into an existing cookie banner.
- **“Opt-in”**: Less widely used, some websites already offer active options for the user to allow or block cookies and tracking before entering a site and to actively make appropriate settings.
- **“Agent system”**: An agent is generally understood to be software that acts partially or fully autonomously in the sense of a user. You could negotiate the privacy settings with the provider when entering a website. A user would only have to define this once and could change it continuously.

In the following, these solutions are discussed in the sense of a scenario analysis [34, 72] from a legal and user perspective and make suggestions for practical solutions.

5.1.1 The Legal Point of View

Regarding “how” to inform (and obtain consent), different ways are now conceivable and to be discussed. The three options already announced above will now be examined in more detail.

With regard to the **cookie banner 2.0**, two different implementations have to be distinguished: First, informing banners that solely seek to raise awareness about use of trackers, and second, banners offering an opt-in.

As an advantage of informing banners, they ensure that the user receives information about the data collection at a prominent position on the respective page. The information can be provided without disturbing the design of the page and its functions, in various forms (text, image, audio,...) and to the extent required in the individual case. A disadvantage, however, is that no legally binding consent can be obtained in this way, as this must

be explicit and, above all, verifiable. Such informing banners, however, only show a notification, without providing options to users. It should also be noted that it is a declared aim of the ePrivacy Regulation to significantly reduce the number of such banners [67]. In summary, an informing banner is at least not a useful instrument in the case of obtaining a consent since it does not fulfil the requirements of data protection for legally valid consent. However, theoretically, an information banner could be legal, if the data processor would not choose to rely on the legal basis of an informed consent, but e.g. on legitimate interests. Since the legitimacy of these interests, currently is a case-by-case decision, for most players, it does not form a viable way to go. In this vein, legal certainty about truly legitimate interests for data processing (e.g. by means of standardization) would be highly valuable.

In contrast to an informing banner, an **opt-in solution** offers the possibility of obtaining verifiable consent. Depending on the design of the banner (e.g. if it is given a size that covers the page content and thus forces users to deal with) and as long as it is technically guaranteed that the data collection actually takes place only after an opt-in has taken place, this solution can initially be regarded as advantageous: It is put in the user's hands whether tracking takes place. However, this initially advantageous characteristic can be turned into a disadvantage relatively quickly. Because against the background of the (increasing) data monetarization (service against data) it is to be doubted that the prohibition of coupling anchored in art. 7 para. 4 GDPR (i.e., the performance of a contract and declaration of consent should not be linked with each other) works [38]. It rather is to be expected, that the user feels urged to the consent, to be able to see the respective contents, and consent without informing further about the background or implications. This would at least cast strong doubt on the information and voluntariness of such consent.

In the jurisprudential discussion, software **agent systems** are rarely present. An exception is a model of having the browser act on user behalf as envisaged in the draft of the future ePrivacy Regulation [67]. According to the model at this draft stage, the user should set up all data protection preferences once when (re-)installing a browser, to have them communicated when browsing a page and thus have any unwanted trackers blocked directly. From a legal perspective, the approach brings the advantage of an effective and high level of data protection. Additionally, user sensitivity to data protection is also "forced" since the user would have to deal with the principles of data protection

and data collection in the network (including cookies and tracking) when setting up the browser.

However, there are also disadvantages to this model: First, the agent would not leave room for a possibly existing legitimate interest of using trackers. Additionally, browser settings can only cover a part of the necessary consents anyway – quasi "general settings". Moreover, individual cases, such as information required for informed consent to a specific data collection, cannot be taken into account. Accordingly, in such cases, cookie banners or similar solutions would again be required, to inform users (and are explicitly provided for in a proposal by the European Commission). To ensure that the use of tracking subsequently also functions technically, an exception rule must be set in the browser within the scope of this consent. This setting must be made manually by the user. As a result, it is to be feared that an effect will occur that is contrary to increasing the level of data protection, in that most users generally allow third-party tracking in their browser settings to be spared annoying requests for the permission of a banner [67]. A partial invalidation of this argument is the result of our study, which showed huge concentrations of ad networks: Almost a quarter of all trackers were assigned to Google, while a large proportion of trackers specializing in visitor behaviour analysis and the sale of personalized advertising were assigned to Facebook. A solution that is not based on a page-by-page control could therefore adopt the users' preferences for trackers of these companies, to cover a large proportion of the potential requests.

5.1.2 The User Point of View

From the user's point of view, a solution modelled on the **cookie banner** cannot be considered an effective [62] or satisfying [45] tool for privacy management. In addition, banners only provide basic information, as Leenes and Kosta [44] have shown. Moreover, even if they are to be understood as a warning over the website to be displayed, such banners show strong signs of wear in terms of their ability to attract attention [12]. Although these facts play into the hands of the operators of the site, effective information or control hardly takes place [19]. Especially, banners do not leave users with choice. The idea of allowing data collection and processing without consent, if relying on legitimate interests could make an interesting debate. The acceptable forms of processing as users perceive them, would have to be researched in-depth to avoid involuntary disclosure, and find viable middle ways.

An apparently quasi-logical extension would be a page-by-page **opt-in solution** for privacy settings. The formal-legal information would have to be confirmed before entering the page. A control would thus be very finely possible so that a user could represent privacy needs quite exactly depending on the implementation – at least page-specific trackers could be rejected. However, analogous to the first case, it should be noted that with the current distribution of tracking, context-dependent individual case regulation by the user will be virtually impossible to manage in an informed manner. Opting in has already shown to lead to fatigue, possibly not least because managing privacy on every single page stands in the way of the users' immediate goal of entering a page [12].

As a reaction, online advertising alliances have already come up with pages where users can manage their tracking preferences for all respective alliance members. However, these preferences also are demanding in terms of both user trust into the alliance member's self-commitment.

Moreover, Utz et al. [76] for example, have presented and compared design options, showing e.g. how nudging strategies are used to manipulate users in their choice. Among general criticism towards the concept of rational choice [27], the applicability of nudging unveils the limits of rational decision-making by individuals.

To avoid this danger and still communicate the needs of privacy for every visited site, a technically more complex solution could be to deliver **software agents** [30] that reside at the user end. To avoid additional software, it would be a good idea to embed such management support in the browser, so that every user has the possibility to make privacy settings without further action, as envisioned by the ePrivacy regulation.

While the design of such tools remains open at present, studies have shown that users are quite willing to accept context-dependent tracking [52], providing room for negotiation on both ends. Currently, however, this leeway is greatly reduced by providers, by essentially forcing a binary selection. P3P offers some experiences in automatically handling privacy on websites [17, 68] by offering companies the opportunity to provide information about the privacy of the user on the respective website voluntarily. Based on such machine-readable protocols, agent systems could act and negotiate privacy between users and operators. These could either apply defined rules or in the form of negotiation processes between the user and the provider of the site, partially autonomous and based on a basic profile and self-learning systems, make decisions for the user. In this scenario, however, prototypical settings would be used, so that no individual case assessment

would be available for the user. In addition, such agents would possibly limit the acceptance of personalized advertising and any tracking very much and possibly also damage legitimate refinancing models of website operators.

5.2 On Informing Data Subjects: A Common Pre-Condition for All Three Former Options

Irrespective of which option is actually applied, a common pre-condition is that users are correctly informed about the data processing. However, the analysis of trackers shows that the current information of users, in particular, about the consequences of the data processing is far from being legally complete. It furthermore is, as the famous example of attitude-behavior-gap [2, 20] shows, a practical problem that is both relevant in research and practical implementation: How can data subjects be informed when abstract data is collected, processed and distributed in large quantities and often in the background?

User research in the field of personalised advertising shows that, in addition to the collection, the handling of forwarding and storage time is important for users in order to regulate the disclosure of data [46]. In addition, it is often important for users what information is obtained from the shared data, i.e. what becomes known about it [33]. With this in mind, the sample obtained shows a significant lack of making data collection visible: Overall, in the vast majority of cases, without additional software, no information about the circumstances of tracking were provided at all. Retention periods were often not disclosed, and service granted themselves far-reaching rights to pass on personal data to third parties. In the field of usable privacy, there already are some guidelines that address the question of how to achieve information and thus transparency in data processing [59, 64].

Designing in a way, such that users learn about data and its underlying information, to make better decisions in similar scenarios by being able to assess the sensitivity of data to be disclosed, is less researched. One approach that oriented towards educating users on the matter of privacy originating from library sciences and pedagogy, aims at the production of "data literacy" [29, 39]. Its methods and concepts are increasingly transferred to other contexts [48, 49], including those of privacy management [33, 35]. For example, feedback systems and dashboards are researched for the potential to educate users about the information content of data and system behavior [32, 47, 59].

These seek to enable users to connect with and better implement their privacy management practices. An example of a possible implementation of such privacy management systems with a focus on the presentation of risks from the user perspective is shown by Jakobi et al. [33] in their study on Usable Privacy in Smart Metering.

From a legal perspective, the risk-based approach anchored in the GDPR corresponds to these findings. Art. 25 GDPR requires data controllers to implement the requirements, such as the principle of transparency under Art. 5 sect. 1 no. 1, and the information duties under Art. 12–14 GDPR, in a way that effectively protects the data subjects (i.e. users) against the processing risks. Thus, the provided information only protect users effectively if they can really understand the information. This goal may only be achieved if such information (e.g. about the collected data, processing purposes and retention periods) gets standardized. The reason for this is that only such standardized information avoids that users have to start, for each particular case again, for the provided information really means and which kind of processing is entailed.

5.3 Synopsis

Overall, an approach based on agent systems seems to be most promising given the legal necessity for consent and the resulting burden for users to manage said consent. Agents offer the possibility to articulate privacy needs without requiring continuous management on a page-by-page-basis or lacking a consent mechanism and merely remaining on an informative level. The setup of an agent also is not necessarily in direct conflict with a current action goal (to visit a website), but could be both part of the setup process of a browser, and continuously available for redesign.

The interactional design and the possibilities for negotiation between parties, however, will be vital for success of such a system. If both users and operators do not offer any leeway, then such an approach will also run into vain to the effect that web pages could introduce tracking-walls analogously to pay- or adblock-walls. For even if there is a prohibition on linking, many website operators are de facto financed by personalised advertising [21].

A bridge in this respect could be the offer of non-personalised advertising as “compensation”, or monetary compensation as mediation. However, pursuing this alternative poses entirely new challenges [19]. Not only would the question of reasonable pricing in relation to otherwise disclosed data be reopened. Moreover, such a deci-

sion could also lead to a division of society in that privacy on the web becomes a luxury good that has to be bought for money.

In each case, a necessary pre-condition for all solutions seems to be that the information of users about the data processing gets standardized, to generate reproducible and therefore predictable outcomes for all parties involved. This is one important step to make users intuitively understand such information, and provide legal certainty, for providers for example, when relying on “legitimate interest” instead of seeking user consent.

6 Conclusion

This article outlined the current data collection practices of popular web trackers. It shows that web tracking remains ubiquitous even after the introduction of the GDPR. Collection, processing and transfer of personal data to third parties by such trackers is common and still largely withdrawn from the attention of users. In light of renewed and evolving legal conditions, unveiling these circumstances and discussing them from a user perspective opens up a design space for improved privacy management in tracking. It shows that agent systems offer advantages from a user and legal viewpoint, but lack research, in particular with regard to the design of mechanisms for negotiation between users and website operators or ad-networks. In future research, a comparison of the design space (cookie banner 2.0, opt-in and agent systems) with regard to the acceptance of the user should be conducted, to be able to inform regulation (such as with the yet-to-come ePrivacy regulation) as well as jurisprudential practice and designers, with empirically validated insights from the user’s perspective.

A data protection-compliant retention of the status quo seems practically impossible in view of the extensive information duties; at least not as long as trackers are used in masses on pages. However, arguably, this use of numerous trackers – as shown above – is not due to technical reasons, but rather to a business decision – surveillance capitalism [79]. However, a major step to make such information duties meaningful for users could be to standardize them. On a standardized basis, users might make their decisions on whether to reveal their personal data for certain data usages or not more in line with their protection goals. These standards, again, would pose a whole new playing field for usable privacy research.

References

- [1] Achara, J. P. et al. 2016. Mytrackingchoices: Pacifying the ad-block war by enforcing user privacy preferences. arXiv:1604.04495.
- [2] Ajzen, I. and Fishbein, M. 1977. Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin*. 84(5), 888–918. DOI:10.1037/0033-2909.84.5.888.
- [3] Akkus, I. E. et al. 2012. Non-tracking web analytics. In: *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, 687–698.
- [4] Angulo, J. et al. 2012. Towards usable privacy policy display and management. *Information Management & Computer Security* 20(1), 4–17.
- [5] Balebako, R. et al. 2015. The Impact of Timing on the Salience of Smartphone App Privacy Notices, 63–74.
- [6] Beales, H. 2010. The value of behavioral targeting. *Network Advertising Initiative* 1.
- [7] Becker, M. 2017. Ein Recht auf datenerhebungsfreie Produkte. *JuristenZeitung* 72(4), 170–181.
- [8] Bitkom e. V. 2018. *Stellungnahme. Zur Positionsbestimmung der Datenschutzkonferenz vom 26. April 2018 zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018*.
- [9] Brecht, F. et al. 2012. Communication anonymizers: personality, internet privacy literacy and their influence on technology acceptance. In: *ECIS*, 214.
- [10] Bujlow, T. et al. 2017. A survey on web tracking: Mechanisms, implications, and defenses. *Proceedings of the IEEE* 105(8), 1476–1510.
- [11] Bundesregierung mit Schreiben des Bundesministeriums für Wirtschaft und Energie 2018. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Ulla Jelpke, Dr. Alexander S. Neu, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 19/5699 – Verhandlungen über den Datenschutz in der elektronischen Kommunikation (ePrivacy-Reform). *Bundesanzeiger Verlag GmbH*.
- [12] Burgess, M. 2018. The tyranny of GDPR popups and the websites failing to adapt. *wired.co.uk*.
- [13] Calo, R. 2013. Digital Market Manipulation. *George Washington Law Review*, forthcoming.
- [14] Clarke, N. et al. 2012. Towards usable privacy policy display and management. *Information Management & Computer Security*. 20(1), 4–17.
- [15] Clifton, B. 2012. *Advanced web metrics with Google Analytics*. John Wiley & Sons.
- [16] Cookie Hinweis: Benötigt jede Webseite einen Cookie Hinweis? <https://www.e-recht24.de/artikel/datenschutz/8451-hinweispflicht-fuer-cookies.html>. Accessed: 2019-04-05.
- [17] Cranor, L. F. 2002. *Web privacy with P3P*. O'Reilly Media, Inc.
- [18] Datta, A. et al. 2015. Automated experiments on ad privacy settings. *Proceedings on Privacy Enhancing Technologies* 2015(1), 92–112.
- [19] Degeling, M. et al. 2018. We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. arXiv:1808.05096.
- [20] Dienlin, T. and Trepte, S. 2014. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*.
- [21] Englehardt, S. and Narayanan, A. 2016. Online tracking: A 1-million-site measurement and analysis. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1388–1401.
- [22] ePrivacy-Verordnung: <https://cms.law.de/deu/insight/e-privacy>. Accessed: 2020-01-15.
- [23] Ermakova, T. et al. 2018. Web Tracking – A Literature Review on the State of Research.
- [24] Europäische Kommission 2017. *Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)*.
- [25] European Parliament and the Council 2016. *REGULATION (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*.
- [26] Felt, A. P. et al. 2012. Android permissions: User attention, comprehension, and behavior. In: *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 3.
- [27] Gigerenzer, G. and Goldstein, D. G. 1996. Reasoning the fast and frugal way: models of bounded rationality. *Psychological Review* 103(4), 650.
- [28] Greengard, S. 2012. Advertising gets personal. *Commun. ACM* 55(8), 18–20.
- [29] Gummer, E. and Mandinach, E. 2015. Building a conceptual framework for data literacy. *Teachers College Record* 117(4), n4.
- [30] Hiremath, P. N. et al. 2019. MyWebGuard: Toward a User-Oriented Tool for Security and Privacy Protection on the Web. In: *International Conference on Future Data and Security Engineering*, 506–525.
- [31] Internetpenetrationsrate weltweit 2021 | Prognose: <https://de.statista.com/statistik/daten/studie/369362/umfrage/prognose-der-internetpenetrationsrate-weltweit/>. Accessed: 2019-04-05.
- [32] Jakobi, T. et al. 2018. Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2(4), 171. DOI:10.1145/3287049.
- [33] Jakobi, T. et al. 2019. It's About What They Could Do with the Data: A User Perspective on Privacy in Smart Metering. *ACM Trans. Comput.-Hum. Interact* 26(1), 2. DOI:10.1145/3281444.
- [34] Jakobi, T. et al. 2018. Privacy-By-Design für das Connected Car: Architekturen aus Verbrauchersicht. *Datenschutz und Datensicherheit - DuD* 42(11), 704–707.
- [35] Jakobi, T. et al. 2017. Providing smartphone data visualizations to support Privacy Literacy (Paris, 2007).
- [36] Joinson, A. N. et al. 2010. Privacy, trust, and self-disclosure online. *Human-Computer Interaction* 25(1), 1–24.
- [37] Kang, R. et al. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In: *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 39–52.
- [38] Klug, C. and Golar, P. 2018. Die Entwicklung des

- Datenschutzrechts im ersten Halbjahr 2018. *NJW* 36, 2608–2611.
- [39] Koltay, T. 2017. Data literacy for researchers and data librarians. *Journal of Librarianship and Information Science* 49(1), 3–14.
- [40] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder 2018. *Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018*. Datenschutzkonferenz.
- [41] Kontaxis, G. and Chew, M. 2015. Tracking protection in Firefox for privacy and performance. arXiv:1506.04104.
- [42] Kranig, T. 2019. *Digitale Dienste im Datenschutzcheck*. Bayerisches Landesamt für Datenschutzaufsicht.
- [43] Krishnamurthy, B. and Wills, C. E. 2006. Generating a privacy footprint on the internet. In: *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*, 65–70.
- [44] Leenes, R. and Kosta, E. 2015. Taming the cookie monster with Dutch law – a tale of regulatory failure. *Computer Law & Security Review* 31(3), 317–335.
- [45] Leon, P. et al. 2012. Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 589–598.
- [46] Leon, P. G. et al. 2013. What matters to users?: Factors that affect users' willingness to share information with online advertisers. In: *Proceedings of the Ninth Symposium on Usable Privacy and Security*, 7.
- [47] Lim, B. Y. et al. 2009. Why and why not explanations improve the intelligibility of context-aware intelligent systems. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2119–2128.
- [48] Markham, A. 2018. Critical pedagogy as a response to datafication: Research methods as data literacy tools. *Qualitative Inquiry*, 25(8), 754–760.
- [49] Markham, A. 2019. Taking the methods classroom to the street: Reflexive qualitative methods to find better prompts for data literacy. *Qualitative Inquiry*, 1–17.
- [50] Mayer, J. R. and Mitchell, J. C. 2012. Third-party web tracking: Policy and technology. In: *2012 IEEE Symposium on Security and Privacy*, 413–427.
- [51] McDonald, A. M. and Cranor, L. F. 2010. Americans' attitudes about internet behavioral advertising practices. In: *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society*, 63–72.
- [52] Melicher, W. et al. 2016. (Do Not) Track me sometimes: users' contextual preferences for web tracking. *Proceedings on Privacy Enhancing Technologies* 2016(2), 135–154.
- [53] Merzdovnik, G. et al. 2017. Block me if you can: A large-scale study of tracker-blocking tools. In: *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, 319–333.
- [54] Nithyanand, R. et al. 2016. Adblocking and counter blocking: A slice of the arms race. In: *6th USENIX Workshop on Free and Open Communications on the Internet (FOCI '16)*.
- [55] Priebe, A. 2018. Was nach der DSGVO-Panik bleibt: Kreative Strategien zur Einholung des Consents. *OnlineMarketing.de*.
- [56] Pugliese, G. 2015. Web Tracking: Overview and applicability in digital investigations. *it - Information Technology* 57(6), 366–375.
- [57] Pujol, E. et al. 2015. Annoyed users: Ads and ad-block usage in the wild. In: *Proceedings of the 2015 Internet Measurement Conference*, 93–106.
- [58] Purcell, K. et al. 2012. Search engine use 2012.
- [59] Raschke, P. et al. 2017. Designing a GDPR-Compliant and Usable Privacy Dashboard. In: *IFIP International Summer School on Privacy and Identity Management*, 221–236.
- [60] Roesner, F. et al. 2012. Detecting and defending against third-party tracking on the web. In: *Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation*, 12.
- [61] Sakamoto, T. and Matsunaga, M. 2019. After GDPR, Still Tracking or Not? Understanding Opt-Out States for Online Behavioral Advertising. In: *2019 IEEE Security and Privacy Workshops (SPW)*, 92–99.
- [62] Sanchez-Rola, I. et al. 2019. Can I opt out yet?: GDPR and the global illusion of cookie control. In: *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 340–351.
- [63] Sanchez-Rola, I. et al. 2017. The web is watching you: A comprehensive review of web-tracking techniques and countermeasures. *Logic Journal of the IGPL* 25(1), 18–29.
- [64] Schaub, F. et al. 2015. A design space for effective privacy notices. In: *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, 1–17.
- [65] Schaub, F. et al. 2016. Watching them watching me: Browser extensions impact on user privacy awareness and concern. In: *NDSS Workshop on Usable Security*.
- [66] Schelter, S. and Kunegis, J. 2018. On the ubiquity of web tracking: Insights from a billion-page web crawl. *The Journal of Web Science* 4(4), 53–66.
- [67] Schleipfer, S. 2017. Datenschutzkonformes Webtracking nach Wegfall des TMG. Was bringen die DS-GVO und die ePrivacy-Verordnung? 10/2017, 460–466.
- [68] Schwartz, A. 2009. Looking back at P3P: lessons for the future. *Center for Democracy & Technology*, https://www.cdt.org/files/pdfs/P3P_Retro_Final_0.pdf.
- [69] Seufert, A.-M. and Vitt, N. 2019. Medien zur DSGVO: Die Berichterstattung vor und seit dem Stichtag im Vergleich. *Wirtschaftsinformatik & Management*, 1–9.
- [70] Sørensen, J. and Kosta, S. 2019. Before and After GDPR: The Changes in Third Party Presence at Public and Private European Websites. In: *The World Wide Web Conference*, 1590–1600.
- [71] Spindler, G. and Schmitz, P. 2018. *Telemediengesetz: TMG mit Netzwerkdurchsetzungsgesetz (NetzDG)*. C. H. Beck.
- [72] Stevens, G. et al. 2014. Mehrseitige, barrierefreie Sicherheit intelligenter Messsysteme. *Datenschutz und Datensicherheit* 38, 536–544.
- [73] Trudeau, S. et al. 2009. The effects of introspection on creating privacy policy. In: *Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society*, 1–10.
- [74] Turow, J. et al. 2009. Americans reject tailored advertising and three activities that enable it. *SSRN*. DOI:10.2139/ssrn.1478214.
- [75] Ur, B. et al. 2012. Smart, useful, scary, creepy: perceptions of online behavioral advertising. In: *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 4.
- [76] Utz, C. et al. 2019. (Un)Informed Consent: Studying GDPR Consent Notices in the Field. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (New York, NY, USA, 2019)*, 973–990.

- [77] Wittig, P. 2000. Die datenschutzrechtliche Problematik der Anfertigung von Persönlichkeitsprofilen zu Marketingzwecken. *Recht der Datenverarbeitung* 2, 59–62.
- [78] Yu, Z. et al. 2016. Tracking the trackers. In: *Proceedings of the 25th International Conference on World Wide Web*, 121–132.
- [79] Zuboff, S. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.
- [80] European Court of Justice. 2019. *Judgment of the Court (Grand Chamber) of 1 October 2019 (request for a preliminary ruling from the Bundesgerichtshof — Germany) — Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*. Technical Report #C-673/17 ECLI:EU:C:2019:80, Rdnr. 13.
- [81] European Court of Justice. 2019. *Judgment of the Court of Justice in Case C-40/17 Fashion ID*. Technical Report #No 99/2019.
- [82] European Court of Justice. 2019. *Judgment of the Court of Justice in Case C-673/17 Planet49*. Technical Report #No 125/2019.
- [83] 2019. *Transport, Telecommunications and Energy Council (Telecommunications) - December 2019, Press conference – Part 4 (Q&A)*.