Online tracking: Questioning the power of informed consent

Eijk, N. van, Helberger, N., Kool, L., Plas, A. van der, Sloot, B. van der

Paper prepared for ITS, 22nd European Regional ITS Conference
Budapest, Hungary, 18-21 September, 2011

Abstract

Online tracking technologies have raised considerable concerns regarding privacy and the protection of personal data of users. In order to help users to regain control over their personal data, Europe has amended its ePrivacy directive towards an opt-in regime. There are however many open questions concerning its implementation, especially regarding the issue of informed consent. This paper explores how the new legal situation impacts on behavioral advertising practices via the storing and reading of cookies in the Netherlands. The results show that the majority of the surveyed parties involved in behavioural advertising do not inform users about the storing of cookies or the purposes of data processing of the subsequently obtained data, neither do they have obtained users' consent for the storage of cookies. We also found that the majority of users lack the skills and knowledge how to handle cookies. These findings critically question the wisdom of the "informed consent regime" which lies currently at the heart of Europe's ePrivacy directive.

1 Introduction

Tracking technologies follow the traces of online users, and harvest a rich collection of personal and usage data. Cookies are an invaluable tool for online profiling and targeting, for example in the context of online behavioural advertising and the personalization of services. Personalization can be valuable and convenient for users. Yet, profiling and online tracking come at a high price. Users loose control over their personal data, and involuntarily and often unknowingly throw the doors open to privacy intrusions and new security risks.

In order to further help users to regain control over their personal data, Europe has amended its ePrivacy directive. The directive has moved from an opt-out regime towards an opt-in regime. Anyone who places and reads cookies or other types of tracking technology needs to provide users with clear and comprehensive information about their placing and purpose, and require informed consent from users. Meanwhile, the deadline for the implementation has passed, however, only a few member states have transposed the European rules. Too many open questions about the proper implementation of its rules and nagging doubts regarding their effectiveness to address the problems at hand hamper the process. Among the most pressing questions is how to meaningfully inform consumers about technically complex issues such as the placing and operation of cookies without unnecessarily hampering the operations of the advertisement industry? Is consent given by means of browser settings adequate and sufficient to comply with the legal requirements? How realistic is an informed consent approach in times of information overload and constantly divided attention? And how helpful are the cookie rules to actually address the underlying real issue: the tracking of users that surf, purchase and communicate online, and the use of this data for all kinds of purposes, most of them hidden from the user.

Confronted with these questions, the responsible Dutch Regulatory Authority for the Telecommunications sector OPTA (Onafhankelijke Post en Telecom Autoriteit) has commissioned a study to explore how the new legal situation impacts on behavioral advertising practices via the storing and reading of cookies, and to identify the main dilema's with the implementation of the new European rules. The Dutch case provides a valuable reality check also outside the Netherlands. Even before the amendment of the directive, the Netherlands already had an opt-in system in place. From the Dutch experience important lessons can be learned also for other European countries. Moreover, the Netherlands is not only a country with a high penetration of active internet users (OECD, 2011), these users have proven to be among the more sophisticated and avid participants in the digital economy [1]. An ideal country, one might say, to study how the informed consent principle fares in practice.

This paper reports some of the main findings of the study for the Dutch National Regulatory Authority (Kool et al., 2011). The paper will show that the majority of the surveyed parties involved in online behavioural advertising (OBA) do not comply with the legal regarding informing users about the storing of cookies or the purposes of data processing of the subsequently obtained data, neither do they have obtained users' consent for the storage of cookies. A reason for maybe even greater concern is the finding that the majority of users evidently lack the skills and knowledge how to handle cookies. Many users, moreover, show little awareness of the privacy implications of profiling and data sharing, or the actual scope of targeted advertising that is already taking place now and today. These findings critically question the wisdom of the "informed consent regime" as it is currently championed in the ePrivacy directive, and in the policy discourse more generally.

The paper concludes with reflections about the concrete policy implications of the findings of the study. It will argue, in particular, that the practical benefits for the protection of users' privacy from an opt-in approach are rather limited. It moreover draws attention to the fact that the use of cookies is only a symptom of a far broader and more comprehensive matter, namely how to approach the online tracking of users' personal data and restore users' control over their own information. In the light of the findings of this study it becomes evident that future discussions must concentrate more on the practice of online behavioural advertising as such, and on identifying workable modes of protection. The ongoing discussion in the US but also in European about do-not-track solutions (DNT) is particularly relevant in this context [2].

The paper proceeds as follows: after a brief analysis of the legal situation before and after the adoption of the ePrivacy directive in Europe and in the Netherlands (section 2), section 3 will report about the findings of a survey among the main providers of targeted advertising in the Netherlands to explore the current use of cookies and targeted advertising practices. The questions from the survey were developed in close cooperation with the legal analysis. The questions were designed to explore the level of compliance with existing regulation, respectively to provide insights into the relevant issues in the context of the implementation of the amended rules. Section 4 describes the findings of a qualitative survey among Dutch internet users with the goal to define their level of skills and knowledge, acceptance of and behaviour towards the placing and reading of cookies for OBA. A concluding section (section 5) summaries the main findings and identifies implications for the future policy debate.

2 Legal analysis

Placing a cookie on the computer of an internet user is bound by rules. The two most important legal requirements for the placing of cookies are informing the user and obtaining his consent. The devil sits in the detail, however, and the most pressing questions when interpreting the applicable rules regard the "when" and the "how". The legally correct answers to these "when" and "how" questions have recently been modified due to an amendment of the applicable legal framework, as will be shown below.

2.1 Legal Framework

A. European Framework

The ePrivacy directive of 2002 [3] provides general rules concerning the processing of personal data and the protection of privacy in the electronic communications sector. It may be seen as the lex specialis to the general Data Protection directive [4], which provides non sector specific privacy rules. Article 5 paragraph 3 of the ePrivacy directive contained a provision regarding, among others, cookies. Generally, it held that placing cookies on the computer of an internet user is lawful under two conditions: First, the user was provided with clear and comprehensive information in accordance with the Data Protection directive. This must include, among others, information about the purposes of the processing. Secondly, the user was offered the right to refuse the cookie. Although some believed the

provision to be a so called opt-in rule, in which both information and consent have to be provided before a cookie is placed on a computer, the provisions are commonly interpreted as an opt-out rule. This also means that the information can be provided after the cookie is placed and the user is able to delete the cookie. Furthermore, we note that the provision addresses users. It's scope is therefore not limited to subscribers or owners of the devices on which the cookie is placed.

The Citizens Rights directive of 2009 [5] changed the aforementioned provision to an opt-in rule. It holds that the placing of a cookie is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with the Data Protection directive, inter alia, about the purposes of the processing. This is commonly interpreted as an opt-in provision. The amendment stirred a debate about the form in which consent can be expressed, and the way information is provided. The discussion that followed focused especially on the former question. The ePrivacy directive refers to the Data Protection directive for the definition of consent [6]. According to this definition, 'the data subject's consent' means any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed [7]. However, a recital of the Citizens Rights directive holds that where it is technically possible and effective, in accordance with the relevant provisions of directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application [8]. This recital has initiated a debate about browser settings. Browsers may be installed so that they accept or decline certain or all cookies. However, most of the current browsers are set to accept all cookies, a fact that is, as we will see later, relatively unknown to most internet users and thus undermines the required principle of 'free and informed' consent. More fundamentally, browser settings do not specify between the individual cookies, while the Data Protection directive and consequently the ePrivacy directive require 'specific consent'. Further confusion was created by a declaration of 13 member states which held that the new regulation changed little about the current practice [9]. However, the European Commission [10] and the Working Party [11] argued otherwise.

B. Dutch Regulatory Framework

European directives have no direct effect and need to be implemented into the national legal order. A distinction can be made between so called minimum and maximum harmonization. In case of minimum harmonization, the European framework spells out a minimum set of rules providing a minimum level of legal protection, allowing member states to adopt additional, and also stricter rules. Maximum harmonization means that the European framework provides a maximum set of rules or level of protection; it leaves significantly less room for member states to deviate from the European standard. The ePrivacy directive is usually seen as providing a minimum set of rules, leaving the national legislators room to provide a higher level of privacy protection to their citizens.
The Dutch legislator made use of that opportunity and stipulated in its implementation of the 2002 rules that both information and consent should be provided before the cookie was placed [12]. It thus contained an opt-in procedure, while the European framework at that time still provided for an opt-out rule only.

Nevertheless, the European rules of 2009 have stirred a controversy about how to implement the European rules also in the Netherlands. The original text suggested by the government held that both consent and information needed to be provided before the cookie was placed, while the current reading holds that they may also be provided simultaneously. Furthermore, some members of parliament wanted to implement the additional requirement that the consent given by the user needed to be 'unambiguous', with as underlying logic that this would exclude the possibility of 'browser consent'. This suggestion did not make its way into the final text either. Having said that, the Lower Chamber did adopt an additional provision holding that when cookies are used for gathering, combining or analyzing data about the use of different information services for commercial, charitable or philanthropic purposes, the Data Protection Act [13] is considered applicable. The Data Protection

Act is the national implementation of the Data Protection directive. Although it is commonly agreed upon that by registering users' internet behaviour, personal data is processed and subsequently the Data Protection Act applies, commercial parties used to deny this. This provision clarifies that the use of cookies for data gathering opens up the application of general data protection law. This means among others that the data controller needs to fulfill one of the grounds for data processing, one of which would be 'unambiguous consent'. This would presumably entail that 'browser consent' would not be sufficient to fulfill the legal obligations. Furthermore, it is highly questionable that one of the other grounds for legitimate data processing mentioned in the directive and the Dutch implementation thereof would be applicable. For example, it is unlikely that the commercial interests of the market parties would outweigh the interests of the users in relation to data and privacy protection. The Bill has yet to be approved by the Upper Chamber, which has no power to amend it, only to approve or disapprove of it.

2.2 Legal requirements

There are three important categories of legal requirements for placing a cookie on a computer, relating to information dissemination to the user, consent from the user and further obligations as laid down in the Data Protection directive. These requirements apply with respect to all cookies, except for so called functional cookies, which are instrumental to the service offered to the internet user, such as storing language settings and storing products in a virtual cart by a web shop. These functional cookies are exempted from the requirements laid down in both the European and the Dutch framework. Non-functional cookies are primarily used for behavioural targeting practices and may either be placed by first parties or by third parties. First party cookies are placed by the publisher of the website visited by a person. Third party cookies are placed by third parties through the visited website. The legal requirements for placing a cookie fall on the party putting the cookie on the computer of a user, but if a third party places a cookie via a website, it may seek to enter an agreement with the publisher sharing these obligations. For example, it is more practical for the publisher to inform a user about the placing of cookies on his website, then it is for third parties that are not in control of the website.

Since the Dutch framework is largely an implementation of the European regulation, the latter will serve as starting point. This also enables a better comparison for non-Dutch readers. Where the Dutch situation deviates, it will be mentioned explicitly. It should be mentioned that next to the sector specific regulatory framework, the involvement of the website owner might constitute civil or public law types of responsibilities and liabilities (tort, unfair business practices, accessory to the act). This limits the possibilities of website owners to unilaterally exclude these responsibilities/liabilities.

A. Information requirement

Regarding the duty to inform users about the placing of a cookie, four aspects need to be taken into account: the moment at which the information is provided, the content of the information, the manner in which the information is given and if it is targeted at the right addressee. Firstly, under the new European rules, the information needs to be diffused before or at least simultaneously with the placing of the cookie. In the case a cookie is a so called persistent cookie, which may remain on the computer for over 10 years, in contrast with session cookies that are removed after the computer has been shut down, the Article 29 Working Party has advised that the dissemination of information to the user must be repeated periodically [14].

Secondly, the content of the communication should at least contain information about the purposes of the processing. The Data Protection directive requires furthermore that the information must contain the identity of the controller processing the personal data and must inform the data subject about the recipients or categories of recipients of the data [15].

Thirdly, with regard to the manner in which the information is distributed, the Working Party 29 has stated that it is important for information to be easily accessible and highly visible. This means that information should not be ‘hidden’ in a link at the bottom of a page referring to a vague and unreadable privacy policy. ‘Statements such as "advertisers and other third parties may also use their own cookies or action tags" are clearly not sufficient’ [16]. Preferably, the user should be informed clearly and visibly on the front-page of the site.

Finally, the information must be distributed to the person from whom the information is gathered and processed. Since a cookie is placed on a computer and a computer may be used by several people, the party placing a cookie would need to inform every specific user of the equipment individually.

B. Consent

Consent, too, must be obtained from every data subject individually. As the Working Party 29 points out, this is especially important in relation to minors [17]. If personal data is gathered about children, the controller will need to obtain consent from their parents. Thus, the controller would need to make sure that the consent obtained with regard to the placing of a cookie originates form an adult. Secondly, at a minimum, consent must be obtained from the user before or simultaneously with the placing of a cookie. Like with information about persistent cookies, it could be feasible to renew consent periodically.

Finally, consent should be provided in an informed, free and specific manner. This means that browser settings which by default accept all or most cookies will not suffice to meet the requirements. Whether browser settings can function as legitimate form of consent when they do not have the aforementioned default settings is still a matter of debate, since it provides for generic, rather then the obligatory specific consent.

C. Data Protection directive

The Data Protection directive is applicable when personal data is being processed. While some market parties hold that they do not process any personal data by following users’ internet behaviour, the pending Dutch Bill implementing the Citizen Rights directive clarifies that the use of cookies for gathering, combining or analyzing data about the use of different information services for commercial, charitable or philanthropic purposes falls under the Data Protection Act. The results from the survey show that generally speaking, market parties indeed indicate that they process personal data (See section 3).

Most importantly, the Data Protection directive grants the data subject the right to obtain information from the data controller, such as regarding the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed. He must be able to do so without constraint at reasonable intervals and without excessive delay or expense.Furthermore, the data subject may request the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this directive, in particular because of the incomplete or inaccurate nature of the data. He may request a notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out, unless this proves impossible or involves a disproportionate effort [18]. Finally, the data subject may also object to the processing of his personal data [19]. In this context, it is useful to differentiate between http cookies and other cookies, such as flash cookies, since additional information about removal or correction might be needed with regard to the other then http cookies. Http cookies are seen as the ‘normal’ cookies and can be removed relatively easy via the browser settings. This is different for other kinds of cookies, such as flash cookies. As the consumer survey (see section 4) demonstrates, the existence of flash cookies is relatively unknown to users, as are the means to remove them. Furthermore, flash cookies are sometimes used for illegal practices such as respawning; when a user

deletes his http cookies via his browser settings, flash cookies are used to regenerate the deleted http cookies.

2.3. Conclusion

The new European “cookie rules” , which are currently in the process of implementation in the Netherlands and in other member states, contain obligations relating to information and consent. The main difference between the previous and the new European rules concerns the moment at which information and consent are due, before or after the placing of the cookie. In deviance from the former European framework, the original Dutch implementation held that both information and consent needed to be provided before the cookie was placed. This approach is continued in the pending Dutch implementation, with the addition that the pending bill clarifies that general data protection law applies when cookies are used in a non-functional way.

How both consent and information is given form is still a matter of debate. While legally speaking, the most correct solution would be to use a pop-up screen every time a cookie is placed, containing the required information and asking consent from the user, this solution is little user-friendly, and it tampers with the business models of the commercial parties offering websites and advertisements. On the other hand, it is clear that it is insufficient to gather consent via default browser settings and on the basis of information that is hidden away in vague privacy policies. A middle ground needs to be found.

Part of a solution could be to differentiate between the different types of cookies. For example, it might be conceivable to adopt a lighter regulatory regime for not only functional, but also session cookies. At the same time, third party cookies or flash cookies might merit stricter legal scrutiny, or even a prohibition. A tailor-made approach would be better prepared to find a balance between the user friendliness of the internet, the commercial interests of the businesses and the privacy of the internet users.

3 Level of compliance of BT providers

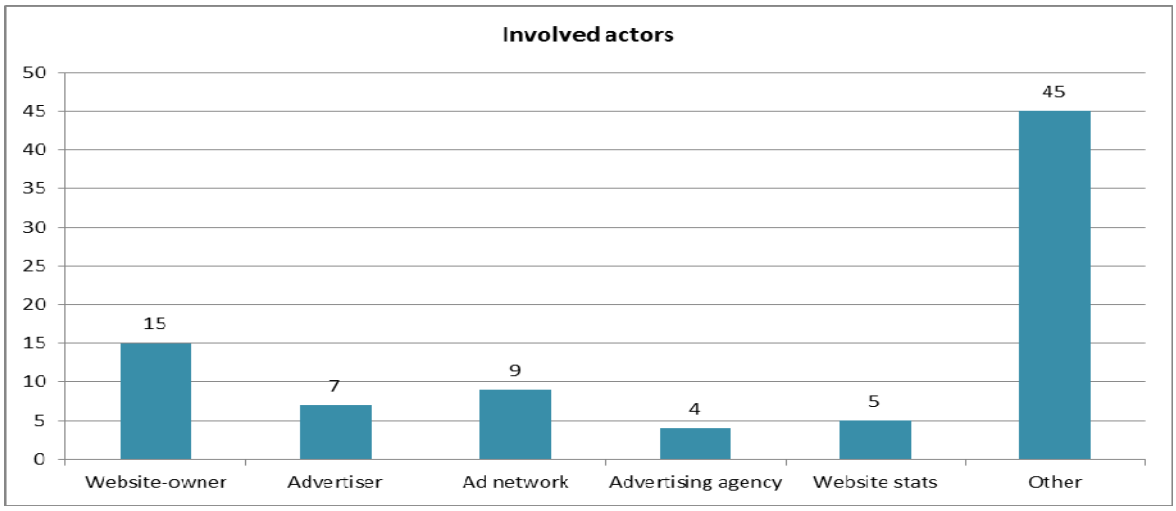
We conducted a survey among the main providers of online behavioural advertising (OBA) in the Netherlands to explore the current situation regarding the use of cookies and to survey to what extent providers comply with current regulation in the Netherlands. The legal analysis described in the previous section identified the main requirements that Dutch providers of behavioural advertising have to comply with. They have been translated into survey questions. A selection of ten main Dutch providers of OBA was made based using three criteria: the most visited websites in the Netherlands, the largest online advertisers in the Netherlands, the web domains with the largest number of visitors. To increase our response rate, the survey was distributed via the Dutch industry organization for marketing and online advertising (Dutch Marketing Dialogue Association, DDMA) and the Dutch industry organization of publishers (Dutch Organization for Publishers, NUV). In total 79 respondents started the survey. Seven respondents did not complete the survey. They were excluded from the results. The number of respondents can vary between questions, as respondents were referred to their following question based on their previous answer. The respondents of the survey are managing directors (n=25), marketing employees (n=16), communication consultants (n=4), compliance officers (n=4), sales managers (n=3), web analysts (n=2) and a mixture of other positions (n=20).

Actors

The results of the survey shows that many different types of actors, which each take on different roles, are involved in delivering personalized ads and contents. A clear value chain can be distinguished, starting with the advertising and ending with the website owner and finally internet users and a range of intermediaries in between, such as advertisement networks, media agencies, affiliate networks and suppliers of website statistics and other tracking technologies. The intermediary parties make it possible for advertisers to tune their advertisements to the behaviour of their visitors

on their own websites and domains, but also to visitors on websites and domains of others. Figure 1 shows the main types of actors that are involved in OBA, such as website owners and publishers, followed by ad networks, advertisers, suppliers of website statistics and media and advertising agencies. In the category 'other' fall affiliate networks, but also charity institutions.

Figure 1: Main activities of respondents



The wide variety of involved actors is also reflected in the way cookies are placed and by whom. The majority of consulted organizations act as a first party; placing cookies themselves, on their own website. But there is a great number of third parties involved; they place cookies on behalf of others, either on their own websites or of websites of others (Figure 2 and 3). Surveyed organizations can thus simultaneously act as both a first party and as third parties. The results show how complex the market for OBA has become, not only for internet users, but also for providers of OBA: who still knows who actually place what cookie, when and where and who is responsible for providing information, obtaining consent and subsequently, for the collected data? In total, 40% of respondents collect data via cookies via a third party, which is used for OBA. In general, website-owners and publishers as well as suppliers of website statistics indicate they mainly act as first party and place their cookies themselves, mostly via their own website. Advertisers, ad networks and media agencies are more likely to act as a third party and let others place cookies on their behalf. Our results are confirmed in a recent study by the Dutch consumer organization which showed that on the majority of popular websites in the Netherlands several third parties are active and place several cookies [20]. Their research showed that that a site with only one first party placing cookies is actually quite rare for popular websites.

Figure 2: Do respondents place cookies themselves and how are cookies placed?

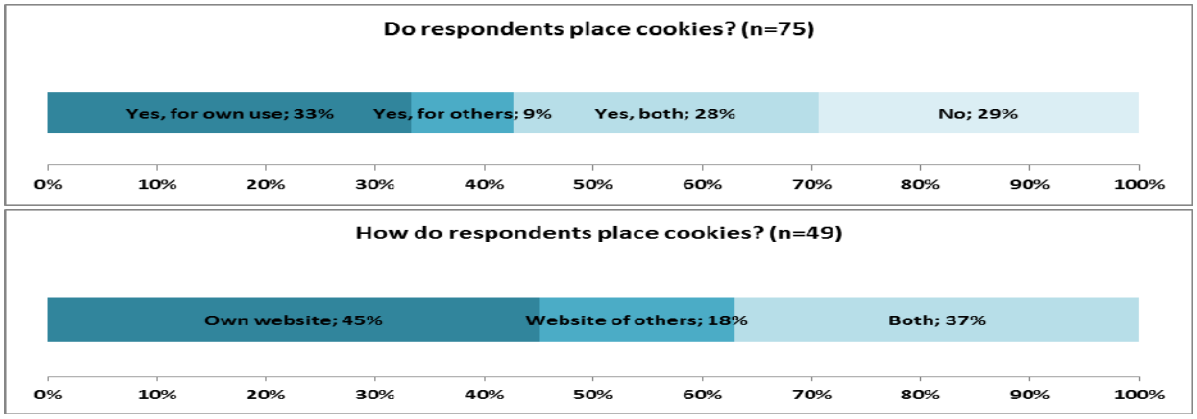


Figure 3: Do respondents let others place cookies and how do they place cookies?

Locations

Table 1 provides an overview of respondents' locations and their ad networks. Respondents are mainly located in the Netherlands and Europe (and fall therewith under European/Dutch jurisdiction), just as their ad networks and the websites on which cookies are placed. Furthermore, the pc's on which cookies are stored as well as the location of data processing is usually the Netherlands (and otherwise Europe). Respondents with their headquarters in the United States also indicate they have an office in the Netherlands.

Table 1: Overview of locations

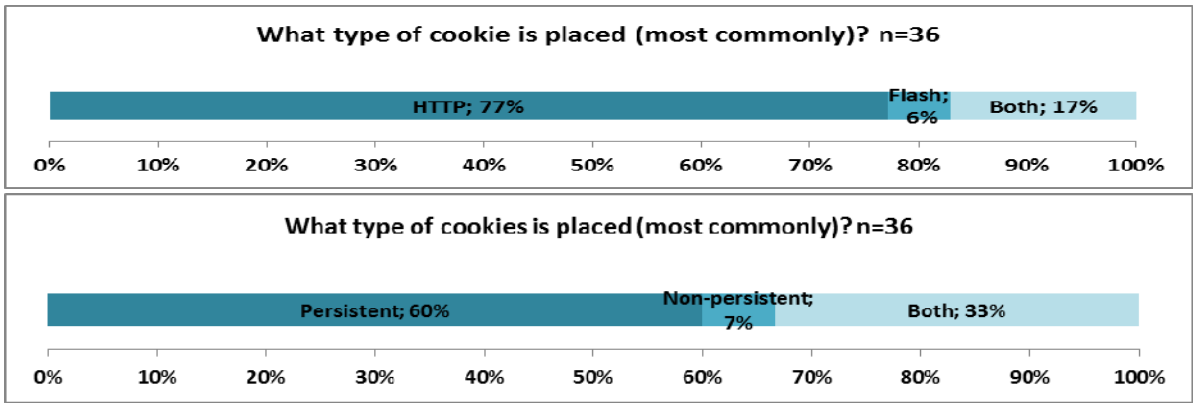
	NL	EU	VS	Other	n.v.t.	n=
Where are websites located that show advertisements?	27	12	5	7		32
Where is the company located that places cookies?	27	8	4	4		32
Where is the third party located?	21	8		3	9	32
Where is the company located to which provide the data?	14	2			14	29
Where is the company located for whom you place cookies?	16	6	1	1	11	28
Where is your firm located?	44	3	1	2		45
Where is your headquarter located?	39	1	4	1		45
Where do you perform your main activities?	43	5	3	4		45
Where is the person responsible for data processing?	37	4	2	2		45
Where are the computers located on which cookies are placed?	39	12	2	1		45
Where are the obtained data processed?	45	6	4	2		45

Cookies

A small majority of respondents places more than one cookie at each page visit. They place between two and ten cookies per visit (the number depends on the type of website and webpage) and they place different types of cookies. The most commonly used cookies are http cookies (see Figure 4). Http cookies can be removed by the user via their browser or via their pc directly. Flash cookies (or Local Shared Objects) are used by websites that use Adobe Flash. Flash cookies cannot removed via browser settings, but via the website of Adobe. In section 4, it becomes clear that users are often not familiar with the existence of Flash cookies, let alone how to remove them. Both http cookies and Flash cookies can either be used for session management, in which case they are automatically deleted once the user closes the browser or they can be used as persistent cookies, in which case

they can remain on the users computer for many years and stay there until users delete them. Respondents indicate that they place cookies for different reasons, such as tracking surfing behaviour of users, authorizing access of users or measuring website statistics and remembering users' preferences.

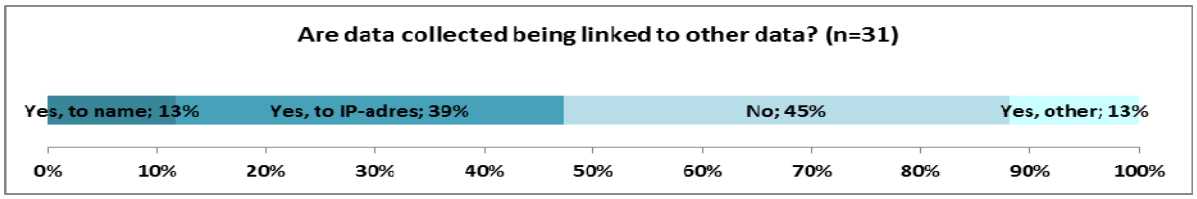
Figure 4: What type of cookies are placed?



Data collection

Only a limited number of respondents indicate to obtain (sensitive) personal data via the cookie directly, such as a users' name, address. However, most respondents (n=24) do link data collected via cookies to other data, such as IP-addresses, name, user name or email (see Figure 5) in order to create more detailed profiles of their visitors and serve their personalized advertisements. This means that in practice, most data can be traced back to specific individuals and may be regarded as personal data.

Figure 5: Data collection



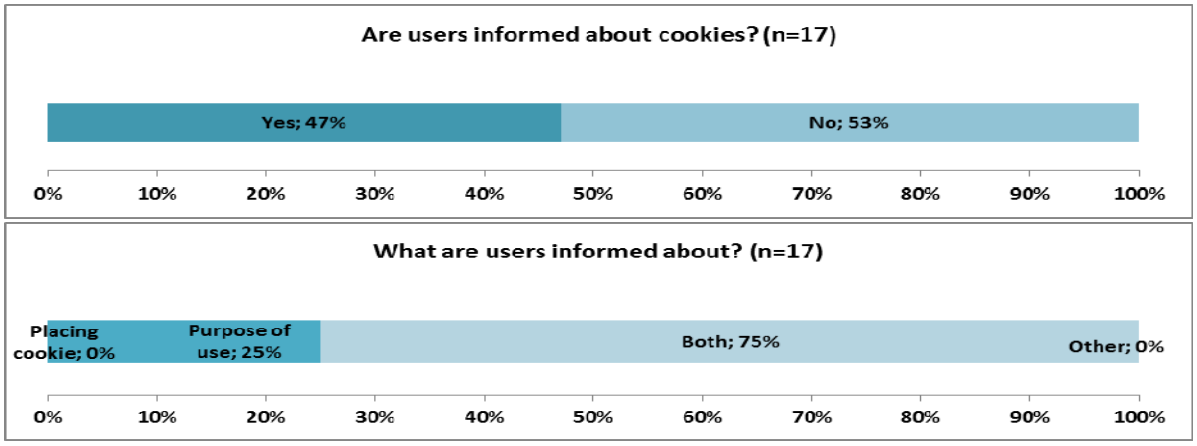
As described in section 2, the amended Directive mentions two exceptions for informed consent: 1) when cookies are necessary for technical storage processes to carry out the transmission of a communication, and 2) when cookies are strictly necessary to deliver a service explicitly requested by the user. In our survey we examined if respondents fall under these exceptions. The majority of the respondents however indicates that data collected via cookies is used for other purposes than these two exceptions. 29% of respondents (9 of 31) indicate they place cookies for the sole purpose of carrying out the transmission of a communication. If asked to describe these purposes, most are found to be in line with the directive, such as remembering language preferences. However, some respondents seem to have a broader interpretation and describe purposes such as creating profiles, providing personalized advertisements and content. With regard to exception 2, five of the remaining 22 respondents indicate that cookie is used for the sole purpose of delivering a service explicitly requested by the user. Again, respondents were asked to describe this purpose. Most respondents describe a purpose that seems to fit the directive (such as storing information in a virtual shopping basket). But here too, broader interpretations can be found, such as showing relevant website content to internet users.

Information

Figure 6 shows that a small majority of respondents (nine of seventeen) currently does not inform users about cookies. They don't inform users about storing cookies on their equipment nor about the purposes for which the cookie is placed. Eight respondents do inform their users, two of which inform users only about the use of data obtained via the cookie, the rest informs the user both about storing the cookie and about how data obtained via the stored cookie will be used. This means that the majority of respondents does not comply with current Dutch regulation. One respondent indicates users are informed *before* the cookies are stored. The others indicate users are informed via privacy policies and general terms of use, after the cookies are stored, which are not easily accessible or understandable for users (see also section 4). Usually, respondents don't take into account that the person which is informed about cookies, is not necessarily the same person from which data is collected.

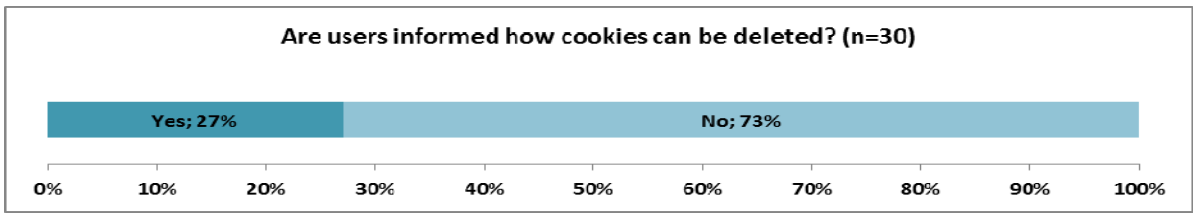
Although the survey results show that different actors are involved in placing cookies on users' equipment (both first and third party cookies), the majority of respondents (10 of 17) have no agreements with other parties with regard to informing users. Nine respondents indicate they do plan to make changes with regard to informed consent due to the amended legislation. However, concrete changes are not mentioned.

Figure 6: Information provided to users



All respondents indicate that it's possible for internet users to delete their cookies, usually via the browser settings. Three respondents indicate that it's possible for users to also delete flash cookies. Although it may be possible to delete cookies, the majority of respondents (73%) does not offer any information to internet users about how to remove them (see **Error! Reference source not found.**). In most cases, cookies that are deleted by users are not restored by other (flash) cookies. However, four respondents admits that this so called *respawning* does occur at their websites.

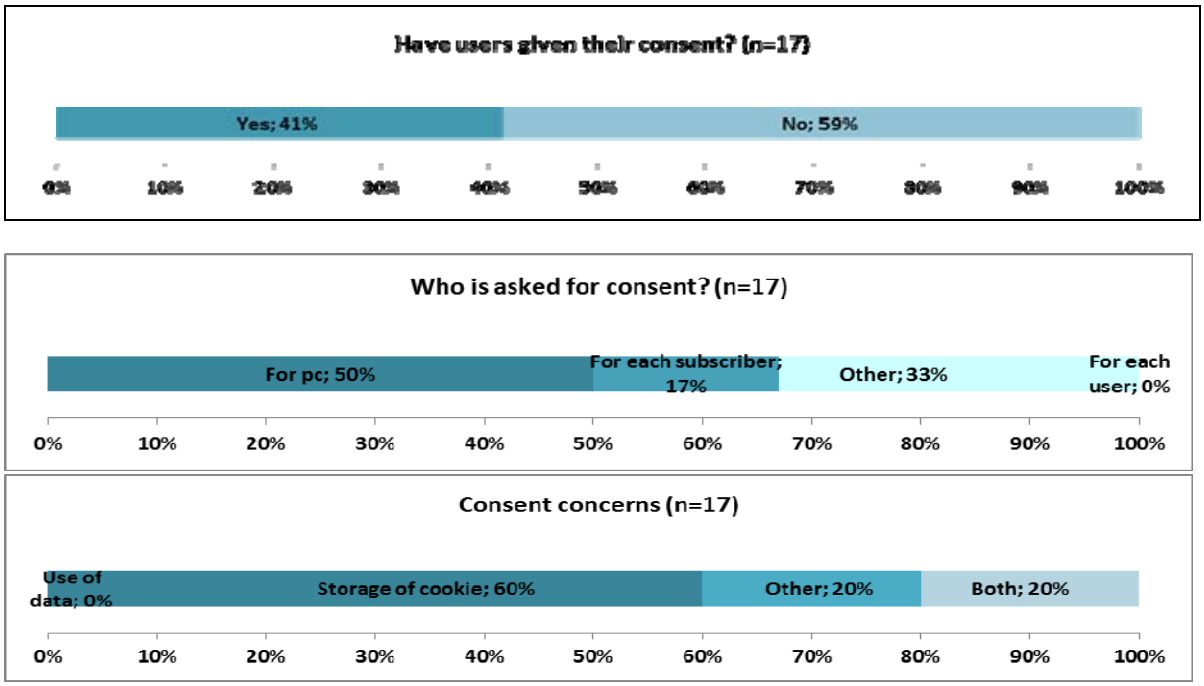
Figure 7: Information about removing cookies



Consent

Figure 8 shows whether respondents have obtained consent from internet users to store cookies. The majority of respondents does not ask consumers for permission to store cookies nor for the use the data that is collected via cookies. Only seven respondents currently ask for permission. Usually, consent concerns storing the cookie on users' equipment. A limited number of respondents obtains consent both for placing the cookie and for the use of data collected via the cookie. However, according to respondents, consent is not explicit, but given by accepting the general conditions or privacy policies of the websites of their clients.

Figure 8: Consent



Data processing

If data collected via cookies concerns (sensitive) personal data, additional legal obligations regarding data processing apply (see section 2). Twenty respondents have indicated to collect personal data. Table 2 provides an overview of data subjects' rights and to what extent respondents respect those rights. None of the respondents comply with all obligations.

Table 2: Overview of compliance with data subjects'

Data subject rights	Yes	No
Access to personal data	8	6
Correction of personal data	7	7
Complete personal data	5	9
Shielding of personal data	8	6
Deletion of personal data	9	5
Corrections submitted to third parties	5	8
Informing DPA	4 (internal officer) 4 (DPA)	6
Processing bound to specific purpose	9	5
Deletion of data after fulfilling purpose	10	4

Most respondents indicate that their data processing is bound to a specific purpose. They provide rather broadly formulated purposes, such as 'easy of use', 'don't show content that users are not interested in' or 'delivering a service'. All respondents indicate that their data processing (the amount of data collected and resulting processes) is in proportion with their specified purpose. Twelve respondents have no agreement with one or more third parties as regard to data procession. Two respondents do have such agreements: one states that suppliers have to comply with their privacy policies, the other states that their client is the owner of the data and that their client is responsible for sufficient guarantees to safeguard the data. They only deliver technical linkages and do not store data from their clients.

Conclusion

The survey shows that a complex network of actors collaborates to deliver OBA (via cookies) to internet users, such as website owners and publishers, advertisers, ad networks and suppliers of statistics and specific software. Actors involved can act both as a first party and as third part,y which makes it difficult to keep track of which actors placed what type of cookie. However, not many respondents have made agreements concerning division of responsibilities of informed consent and data processing.

The majority of respondents indicate they don't inform users or obtain their consent, not about storing the cookie, nor about the use of obtained data. These respondents do not comply with the existing regulation in the Netherlands which raises questions regarding the willingness of the industry to comply with the opt-in rules. If consent is asked, it involves a generic type of consent, for example via browser settings or via general terms and conditions. The majority of respondents also does not inform users about ways that they can remove cookies. Most respondents link obtained data to a (user)name of IP-address, which means that data can often be traced back to specific individuals. But, users' rights with regard to processing of personal data is respected by only half of the respondents. The limited transparency from the side of industry about OBA practices makes it difficult for internet users exercise control over the processing of their data. This is strengthened by the fact that internet users already have limited knowledge of OBA and possibilities of browser settings, as will be shown in the next section.

4 Consumer knowledge and skills regarding behavioural advertising

One of the most critical questions in the implementation of the amended directive is the issue of informed consent. How can and should consent be given? How can consent be implemented in practice? Several browsers offer possibilities to allow or block cookies with different degrees of granularity (for example to block all cookies or to block cookies from third-parties). By default, all browsers are set to automatically accept all cookies. Consent assumes a sufficient understanding and knowledge of internet users to be able to make a substantiated choice. However to what extent are users actually aware of these browser settings, behavioural advertising and the use of cookies? The Article 29 Working Group (2010) is therefore critical about the use of browser settings for informed consent as we have seen in section 2.

Existing literature in the United States suggests that internet users have limited knowledge concerning behavioural advertising. McDonald and Cranor (2009; 2010) find for example that participants in their study have a poor understanding of how OBA works, they don't understand the use of cookies for the purpose of OBA and don't realize that OBA occurs. Research in the United States also suggests users have privacy concerns relating to OBA. A quantitative survey among US citizens found 63% of the respondents is concerned about their online activities are being monitored, once they learn about third party cookies (Wills and Zeljkovic, 2010). MacDonald and Cranor (2010) find that 64% of participants find the idea of OBA invasive and 40% of participants indicate they will change their online behaviour if advertisers would collect their data. The results of Turow et al. (2009) are similar and find that 66% of US citizens do not want that online ads are tailored to their interests.

A recent Eurobarometer study (2011) shows that the majority of European internet users are also uncomfortable with internet profiling and OBA. In the Netherlands, 45% is fairly uncomfortable and 24% is very uncomfortable with OBA. In addition, 70% of European internet users are concerned with companies holding personal information and using that information for other purposes than that for which it was collected (including direct marketing and targeted online advertising) (Eurobarometer, 2011, p. 151). Although the literature suggests users are concerned with online behavioural advertising, studies also shows that their concerns have limited effect on users'browsing and online shopping behaviour (Alrech and Settle, 2007).

For our case study of the Netherlands, we conducted focus group research to explore the level of knowledge of Dutch internet users regarding OBA, cookies and browser settings and their attitudes. Four heterogeneous groups (gender, age, education and internet experience) have been organized. Each focus group lasted two hours. The programme comprised four core elements: 1) attitudes regarding OBA and online privacy, 2) knowledge of OBA and related terms (such as cookies, first party, third party), 3) understanding of privacy policies (relating to cookies), 4) knowledge and skills to set browsers to specific preferences. In total, 32 consumers were invited, of which 6 cancelled. Results have been analyzed for each group and then compared. Results show strong similarities over all four groups.

Attitudes regarding OBA

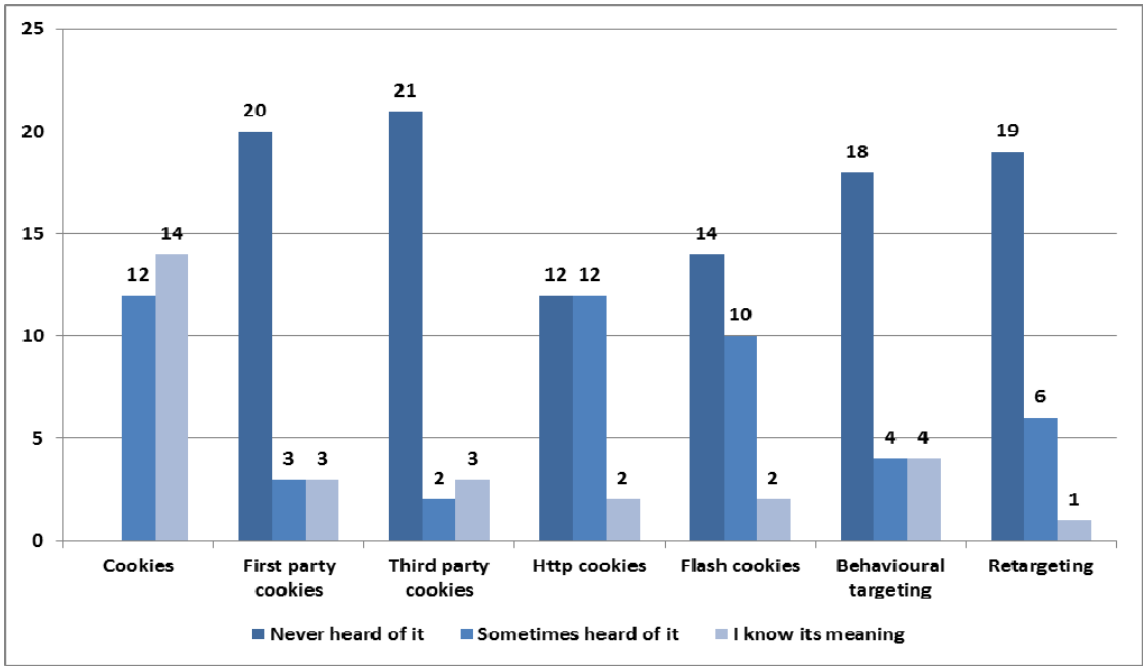
Most participants don't realize that OBA already occurs and believe it is something for the future. When prompted, they indicate that they did notice that some websites behave in a 'smart' way, but did not relate this to their own behaviour or the tracking of their personal data.

"But, you don't receive any personalized advertisements other than in your mail account"
"I don't think it is that far yet, that you can see to it that men don't get advertisements for sanitary towels. I don't think it is that detailed yet."
"I was already wondering, what a coincidence I receive advertisements about the city I live in!"

Knowledge of OBA

Perhaps not surprisingly, participants have limited knowledge of behavioural advertising and related terms. Although all participants are somewhat familiar with the term cookies and most of them can give a description of what cookies are, this description is partial and relates to storing password information or other personal preferences and not to behavioural advertising. Most participants have never heard of more specific types of cookies (such as first and third party cookies, or http and flash cookies). They are also not familiar with the term behavioural targeting or advertising.

Figure 9: Knowledge of OBA and related terms



To explore to what extent users understand privacy policies that discuss the use and purposes of cookies, participants are handed out privacy policies of three popular websites in the Netherlands. Participants indicate they usually don't read privacy policies and explain that the policies are 'standard texts' and for every website or internet service very much the same.

'A privacy policy is standard, once you have read one, you have read them all'

Participants know that companies collect data about their customers, but they are not familiar with the fact that via third parties their data might be shared with others than the owner of the websites they visit. Some participants indicate such data sharing with third parties only happens if they have given their consent, but confuse giving consent for third party cookies with accepting news letters and special offers from third parties by ticking off boxes in the general conditions.

Participants find it important that there is an easy way to opt out of the use of cookies for OBA, but did not know they could find this information could be found in the privacy policy. Some website owners offer their users a possibility to opt-out in their privacy policy, by clicking a link that place a do not follow me cookie on their computer. None of the participants have ever opted out of cookies via privacy policies. Participants find it strange that the companies of the websites they visit don't take responsibility for third party cookies and that they refer uses to the third parties to opt out of their cookies.

"I think the [company website] is responsible for what Third party do with your data, you choose to go the the [company website], you don't choose to got to the Third Parties."

Browser settings

All participants indicate they know use their browser to accept or block cookies. However, when they are actually asked to do so, it turns out to be very difficult for most participants. Only a few participants manage to set their browsers without any help. Most participants need the written guidelines that are handed out after five minutes and some participants need help from the moderators. None of the participants knew how to monitor or delete flash cookies and expect this can be done via the browser as well.

"Now I now how to do this, but by the time I get home, I will not remember."
"You feel like a system administrator, not everyone can do this."

Participants are surprised about the number of cookies that is placed on their computer after five minutes of internet surfing. Participants are now able to identify third party cookies and question their origin.

"I went to website [x], and now I also have a Facebook cookie. <thinks for a moment> The reason must be that 'I like button'
"I have cookies from Ilse media, but I have never search with that. What do they need those cookies for?"
"I think I'm able to trace the origin of maybe five to ten percent of these cookies, but I don't know where the rest comes from."

A number of participants is not concerned about the number of cookies, but most participants feel concerned after the assignment.

"They store something somewhere on your pc, but you don't know what it is."
"It feels like I have opened the front door and everyone can just walk in as it were"

A small number of participants consider themselves responsible to prevent misuse of the data collected via cookies, but most participants consider policy makers, regulating authorities and website owners as responsible actors. The most important reason to put responsibility outside the internet user is that participants don't believe the average internet user is capable of taking well informed decisions regarding cookies.

Conclusion

The results of our focus groups show that participants have limited knowledge of behavioural advertising and cookies. Most participants are familiar with cookies, but don't link their use to OBA. Participants don't realize OBA already occurs, but do express privacy concerns if they were served personalised advertisments. Furthermore, participants have limited skills regarding the use of browser settings to accept or block cookies. Deleting flash cookies is for most participants even impossible. At the moment, most internet users seem unable to make a well-informed and substantiated choice regarding cookies and OBA due to their limited knowledge and limted skills. This lack of knowledge of consumers on the one hand, and the limited transparency of the industry on the other, raises questions regarding the implementation and effectiveness of informed consent.

5. Conclusions

In response to the increasing concern about the online tracking and profiling of users, the amended ePrivacy directive adopted a stricter regulatory framework for the use of cookies. The former opt-out approach has been replaced by an opt-in regime that requires users' consent in combination with the provision of clear and comprehensive information. The findings from a study for the Dutch telecommunications regulator OPTA about the level of compliance with the Dutch opt-in rules, which existed already prior to the amended directive, shed a critical light on the cookie rules, their enforcement and potential value for the protection of users' privacy.

The majority of the surveyed parties neither inform consumers about the placing of cookies, the purpose of the processing of the so won data, and how the cookies can be removed, nor would most of the parties studied require consent from consumers before doing so. These findings question the willingness of the industry to comply with the opt-in rules, at least in the Netherlands, and raise important questions regarding the possible costs and strategies of enforcement and implementation of the new framework, also outside the Netherlands. One may wonder to what extent the low level of compliance can at least in parts be explained by a lack of legal knowledge on the side of the industry, in which case awareness building measures are needed. This is certainly also true with regard to the provisions about the lawfulness of data processing in general data protection law, which fully apply to the processing of data won from cookies. Too often overlooked is the fact that not only the placing of cookies, but also the processing of collected data must comply with privacy law. The pending law Dutch law to implement, among others, the ePrivacy directive further re-enforce that link.

To the extent that providers do inform consumers and ask for consent, this is often done in a way that is little conductive to exercising greater control over their personal data. A quarter of the parties that do inform users only do so with regard to the way the data is used, not about the fact that cookies are placed. Generally lacking or insufficient is also information about the removal of cookies. Such information is particularly crucial in case of flash cookies, HTML5 cookies or other forms of cookies that users are even less familiar with than "normal" cookies. It is worth noting that there is little differentiation in general between the types of cookies or the various purposes for which data is being collected, nor about the concrete implications of profiling and online tracking for users' privacy. Unsatisfactorily is also the visibility of the information, which is often hidden away in lengthy privacy notices or at remote places on a website). These findings beg the conclusion that more concrete guidance regarding the manner and quality of information provision are needed. Standardization might have an important role to play in this context. This is even more so since, as the study showed, users commonly do not expect major differences between the individual privacy polices of the various providers. Another relevant aspect in this context is the need to differentiate between different forms of cookies.

In practice, consent is often 'given' in form of pre-defined browser settings. If a browser is set in a way to accept per default all or no cookies it cannot be said that the user has given informed consent. With regard to more sophisticated browser settings, the consumer survey triggers considerable concern whether the majority of users is actually skilled and educated enough to handle their browsers' settings and block unwanted cookies. It must be noted, moreover, that certain cookies, such as flash cookies cannot be blocked or removed with the browser at all, and only few respondents were actually able to remove these kinds of cookies. The survey also found a lack of awareness of the link between the browser settings and being targeted for advertising. More generally it is relevant to notice that the general awareness with regard to the reality and scope of behavioural advertising is rather limited among most users. In sum, it is very doubtful if consent via generic browser settings is adequate and sufficient to comply with the legal requirements. There is a clear need to investigate more sophisticated solutions such as do-not-track options. Do not track options are currently high on the policy agenda in the US, and also in Europe, where do not track options are gaining in prominence in the policy discussion. As such DNT is much broader than just cookies or other types of

profiling techniques (such as (device) fingerprinting), it addresses the more elementary process of tracking as such.

Another key question that needs more attention is the question of who is responsible for third party cookies, and their compliance with general and sector specific data protection law. Unlike first party cookies, third party cookies are almost never necessary for the functioning of a website but are used for other purposes, including targeted advertising. The concern about the loss of control over users' data and the legitimacy of data processing is accordingly particularly pressing in this context. The users in the survey indicated that they are particularly concerned about the placing of third party cookies and the fact that no party seems to assume responsibility for those cookies or the way they are used to track and process users' data. The user survey found that users put considerable trust in website publishers, also and particularly with regard to third party cookies. The more striking it was to see that there are hardly any agreements among parties about the distribution of responsibilities for the placing of cookies and compliances with the data protection rules. This is particularly true for the question of who is responsible for informing users and requesting consent: the website publisher, advertisers, parties placing third party cookies, etc. Many privacy policies of website publishers do not even refer to third party cookies.

A related conclusion that can be drawn from this study is the need to reconsider the present one-size-fits all approach to the dealing with cookies. While certain cookies, such as sessioncookies, are seldomly the cause of concern for users' or users' privacy, other cookies pose potentially bigger threats to users' privacy. Examples are third party cookies, but also persistent cookies, respawning cookies (which are forbidden), or flash cookies that are more difficult for users to detect or remove. A more risked-based approach to the dealing with cookies seems to be better suited to strike a balance between the interests of users in regaining control over their personal data, and the interests of website holders and the advertisement industry in extracting value from user data.

As a final remark, it is important to keep in mind that the actual issue at hand is broader and more serious than the placing of cookies on users' equipment. At the hearth of the controversy are the implications from online tracking and excessive profiling for users' privacy. New developments, such as 'device fingerprinting' techniques [21] underline this point even more. These techniques no longer store information on users' equipment, but unobtrusively identify users via their unique browser and operating system settings, which make complicates the issue of control over personal data even further. What is needed are initiatives that help users to truly regain control about their personal data, and in a way taking into account their skills and the practical demands of an online environment. Needed is also a clearer understanding of the privacy implications of profiling and behavioural advertising more generally, and the implications for value and design of DNT solutions. This study has demonstrated quite clearly that "informed consent" alone will not suffice in addressing the issue.

Notes

[1] European Travel Commission, New Media Trend Watch, "Netherlands", online available at: http://www.newmediatrendwatch.com/markets-by-country/10-europe/76-netherlands (last visited on 15 July 2011)
[2] See Remarks of FTC Commissioner Julie Brill at the Centre for American Progress, "Privacy: Tracking our Progress with Pomp and Circumstance", June 27 2011, online available at http://www.ftc.gov/speeches/brill/110627capspeech.pdf (last visited on 15 July 2011); N. Kroes, Vice-President of the European Commission responsible for the Digital Agenda, "Online privacy – reinforcing trust and confidence", speech presented at the Berkeley Centre for Law and Technology (BCLT) and Institute for Information Law (IViR) "Online Tracking Protection & Browsers Workshop", Brussels, 22 June 2011, online available at: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/461 (last visited on 15 July 2011).
[3] Directive 2002/58/EC

[4] Directive 95/46/EC
[5] Directive 2009/136/EC
[6] Article 2 sub f e-Privacy Directive
[7] Article 2 sub h Data Protection Directive
[8] Recital 66 e-Privacy Directive.
[9] https://nodpi.org/2009/11/23/uk-and-12-other-member-states-issue-statement-on-telecoms-reform-package/
[10]http://ec.europa.eu/information_society/policy/ecomm/todays_framework/privacy_protection/spyware_cookies/index_en.htm
[11] Article 29 Working Party, 'Opinion 2/2010 on online behavioural advertising', WP 171.
[12] As formulate in article 4.1 of the ministerial decree implementing the provision (Besluit Universele Dienstverlening en Eindgebruikersbelangen).
[13] Wet bescherming persoonsgegevens.
[14] WP 171, p. 21.
[15] Article 10 Data Protection Directive.
[16] WP 171, p. 18.
[17] WP, 171, p. 17.
[18] Article 12 Data Protection Directive.
[19] Article 14 Data Protection Directive.
[20] Consumentenbond (2011) Nederlandse websites zijn koekiemonsters (Dutch websites are cookiemonsters), 31 januari 2011, accessible via http://www.consumentenbond.nl/test/elektronica-communicatie/internet-en-software/veiligonline/extra-informatie/cookies-test/
[21] The Wall Street Journal, Race is on to fingerprint phones, pc's. November 30, 2010, http://online.wsj.com/article/SB10001424052748704679204575646704100959546.html?mod=dist_smartbrief

References

Alreck, P. & Settle, B. (2007) Consumer reactions to online behavioural tracking and targeting, Journal of Database Marketing & Customer Strategy Management (2007) 15, 11–23.

Eurobarometer (2011) Attitudes on Data Protection and Electronic Identity in the European Union. Special Eurobarometer 359. June 2011.

Kool, L., A. van der Plas, N. van Eijk, N. Helberger, B. van der Sloot, "A bite too big: Dilemma's bij de implementatie van de Cookiewet in Nederland", report for the Dutch National Regulatory Authority for the telecommunications sector (OPTA), 28 February 2011.

McDonald, A. and Cranor, L. (2009) An Empirical Study of How People Perceive Online Behavioral Advertising, Carnegie Mellon University.

McDonald, A. and Cranor, L. (2010) Americans' Attitudes About Internet Behavioral Advertising Practices Carnegie Mellon University.

OECD (2011) OECD Broadband Portal. Fixed and wireless broadband subscriptions per 100 inhabitants (Dec. 2010), 23 June 2011, http://www.oecd.org/document/54/0,3343,en_2649_34225_38690102_1_1_1_1,00.html (accessed 14 July 2011)

Turow, J., King, J., Hoofnagle, C., Bleakley, A. and Hennessy, M. (2009) Americans Reject Tailored Advertising and Three Activities that Enable It, University of California, Berkeley, School of Law.

Wills, C. and Zeljkovic, M. (2010) A Personalized Approach to Web Privacy—Awareness, Attitudes and Actions, Worcester Polytechnic Institute.