

Management summary

Introduction

Online advertisement is an important source of revenue for many providers of online services. Internet technology, such as storing and 'reading' cookies on users' computers, enables website owners and/or advertisers to register surfing behaviour and build profiles regarding their preferences. The profiles are used to serve targeted or customized adds to internet users. This is called *behavioural targeting*, *behavioural advertising* or *personal advertisement* and it is an increasingly popular way to offer online advertisements to internet users. While in principle an economically attractive and potentially effective tool, behavioural advertising also raises considerable concerns regarding privacy and the protection of personal data of users.

The recently amended ePrivacy Directive (article 5(3))¹ has triggered controversial discussions in Europe and its member states regarding cookies and more in general regarding behavioural advertising. The ePrivacy Directive created an opt-in regime for storing and 'reading' cookies, requiring the user's consent and requiring that the user has been provided with clear and comprehensive information (in accordance with Directive 95/46/EC) about the purposes of the processing. By the end of May the amended Directive has to be implemented in national law in the European Member States. In the Netherlands, the Directive will be implemented by the Telecommunications Act, for which a bill has been put forward in Parliament.

Research objective

The Dutch telecom regulator OPTA (Onafhankelijke Post en Telecom Autoriteit) has commissioned TNO and IViR to conduct a study to explore how the new legal situation impacts on behavioural advertising practices via storing and reading of cookies. It should be mentioned that the amended Directive regulates the way cookies should be stored, but that storing cookies does not mean that behavioural advertising occurs, and vice versa, behavioural advertising does not always occur via storing and reading cookies. This report will present the results of the study. It provides an indication of current behavioural advertising practices via cookies and identifies the main questions regarding the implementation of the amended directive. The study shows that there is still a long way to go before the new regulation can be successfully implemented.

Approach

The study was carried out between November 2010 and January 2011. During this period, the following activities have been carried out:

- We have performed a legal analysis of the current and new regulation in the Netherlands concerning the storing and reading of cookies on users' equipment based on desk research (European directives, Dutch regulation and relevant case law) completed with literature research and an analysis of the main stakeholders, such as Article 29 Working Party (Chapter Two).
- We conducted a survey among the main providers of behavioural advertising in the Netherlands to explore the current use of cookies and behavioural advertising practices. The survey is based on the legal analysis. The results indicate the level of compliance with existing regulation and provide insight into relevant issues for the implementation of the new regulation.

¹ Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Results

The survey shows a range of actors that collaborate to offer behavioural advertising (via storing and reading cookies), such as website-owners, advertisers, advertisement networks and suppliers of website statistics). They are mainly located in the Netherlands. Both First Party and Third Party cookies are being used. A limited number of respondents only stores First Party cookies, in order to facilitate communication over the internet (for example by remembering language settings and other personal preferences) or to be able to offer the service as requested by internet users (such as a shopping basket). However, most respondents store Third Party cookies, for example to offer behavioural advertising. 60% of the respondents obtain data for targeted advertisement via an intermediary actor. Remarkably, a small number of respondents (13%) admits that respawning occurs, while this is not allowed in existing law (Article 4.1 of Besluit Universele Dienstverlening en Eidgebruikersbelangen, BUDE, or Decision regarding Universal Services and End Users Interests).

Most respondents link the obtained data from the stored cookie to a (user)name or IP-address. The obtained data can then be traced to an individual. In most cases, the obtained data is used to create profiles. Respondents are not always very transparent about storing cookies for the purpose of behavioural advertising. A small majority (53%) indicates that they don't inform users, not about storing cookies on their computers, nor about the purposes and use of subsequent data processing. The majority (53%) of respondents also do not ask users for permission to store cookies on their computers, or for permission to use the obtained data. If respondents do ask for permission, this usually is a generic consent (for example given via browser setting or by users accepting the general terms and conditions of a website or service).

The results of focus groups show that participants have limited knowledge regarding behavioural advertising and cookies. Although they are familiar with the term cookies and its technical meaning (small text files on their computer), they don't link the term to behavioural advertising. Most participants are not aware that behavioural advertising already occurs. It is difficult for the participants to distinguish between First Party and Third Party cookies, or between http and flash cookies. They lack sufficient knowledge regarding cookies and behavioural targeting to make a sound choice whether he or she wants to accept cookies (for the purpose of behavioural targeting). The limited set of skills of participants is another obstacle in this respect. Setting up the browser in such a way to block http cookies is for most participant a very difficult task. Even more difficult is the task of removing and blocking flash cookies.

Conclusions

In Chapter Two we made an analysis of the legal context. The regulations regarding storing and reading of cookies have changed in Europe from an opt-out to an opt-in regime. This means that the one who stores the cookie is obligated to inform the user before or at the moment the cookie is stored on the users' terminal equipment about the cookie and the purposes for data collection. In addition, he is obligated to ask for permission to store the cookie on a user's terminal equipment. In the Netherlands however, not much has changed as the Netherlands already handles an opt-in regime. Furthermore, complementarity exists between the regulations regarding storing of cookies and the more general regulations regarding data collection and processing, as regulated by the Dutch data protection act. Besides the informed consent issue, providers of behavioural advertising will generally also have to comply with the data protection act.

When the legal analysis is confronted with the empirical results of the study, it becomes clear that the majority of surveyed providers of behavioural advertising do not inform users about storing cookies, and do not inform users about the purposes of data processing of the subsequent obtained data. The majority also does not have the users' consent for storing cookies. The majority of respondents therefore does not comply with existing Dutch regulations regarding the information and consent issue. This calls into question the willingness of providers to comply with the new regulation. In addition, the results from the focus groups among consumers shows that users currently have

insufficient knowledge and skills to make substantiated choices regarding accepting cookies or not (for the purposes of behavioural advertising). The results show how service providers' practices and users' knowledge make two separate worlds, which raises the question whether additional regulation is not almost certainly required.

In addition, the following observations with regard to supervision and enforcement can be made:

1. The need for clearly described responsibilities and roles of involved actors

The survey shows that a wide array of actors is involved in storing cookies for the purposes of behavioural targeting. It should be clear what the roles and responsibilities of all involved parties are with regard to their legal obligations. The survey shows that actors hardly make agreements among themselves concerning the responsibilities of each actor involved. This applies at least to the information and consent obligations, which means that these two obligations are not fully complied with. For example, many privacy statements of website owners do not or only very briefly refer to the use and storage of Third Party cookies. On the other hand, consumers in the focus group indicate that they are concerned precisely about these types of cookies and the fact that website owners do not take responsibility for these types of cookies. In addition, Third Party cookies are not strictly necessary to deliver a particular internet service; the regulations regarding information and consent do also apply to these type of cookies. Third Party cookies also raise questions regarding the data protection act: is there for example an adequate legal basis for data processing? The division and roles of involved actors needs to be more clearly defined.

2. Jurisdiction

Most actors involved in storing cookies for the purposes of behavioural advertising are either located in the Netherlands or Europe. This means that jurisdiction exists, either directly or indirectly, which increases the potential for effective supervision and enforcement.

3. Cookie diversity: towards a tailor-made model?

The results show that involved actors use different types of cookies. Some cookies are stored for the sole purpose of facilitating the visit to the website (such as remembering language preferences or electronic shopping baskets). These types of cookies and, more in general, session cookies raise hardly any privacy or data protection issues - as opposed to persistent cookies, that stay present on the end users terminal equipment. Questions relating to this type of cookie are: a) whether the issue regarding informed consent needs to occur only once or periodically, b) how the data processing over long periods of time relates to purpose specification, purpose binding, proportionality and necessity requirements as laid down in the Dutch data protection act, c) how consent of a data subject can be considered specific and informed if it is not clear in advance which data will be processed and for what purposes. Persistent cookies also problematic when multiple users use the same equipment together. How can the obligations regarding informed consent in such a situation be fulfilled? Should perhaps a limitation to the lifetime persistent cookies be considered? And is differentiation required with regard to the nature of the cookie as (un)familiarity of users varies between different types of cookies or deletion is very complicated (in the case of flash cookies)? A tailor-made approach seems more appropriate than a one size fits all strategy.

4. Limitations and obligations regarding data collection and data processing

The respondents of the survey indicate that many cookies are used for data collection and subsequently data processing. At the same time, actors are insufficiently informed regarding existing legal limitations and obligations as laid down in the Dutch data protection act. Are the obligations regarding purpose specification, proportionality, necessity and data collection fulfilled? Are the rights of data subjects sufficiently respected (for example regarding information about and access to information that is collected and processed about him or her, or correction, completion or deletion of this information and the obligation of data processors to pass on such requests to third parties to which the original data have been given)? In general, this is not the case.

5. Clear conditions for information provision

A small majority of the respondents of the survey does not inform their users. In addition, 25% of the respondents who do inform their users, only informs about the use of the obtained data, not about storing the information or gaining access to it. Furthermore, information about deleting cookies, for example regarding flash cookies, is often missing or very limited. The issue of informed consent is getting more urgent if techniques such as HTML5 will spread more widely. There is hardly any differentiation in the provision information regarding the type of cookie that is stored and for what purposes. Moreover, the way information is provided, usually at the bottom of a website, will be insufficient to comply with the legal requirements. Also, the quality of information, the readability and the accessibility and understandability leaves a lot to be desired for. Most users turn out to be hardly informed about storing cookies for the purposes of behavioural advertising, the way this occurs and what measures they can take to prevent this. Clear conditions with regarding to information provision are called for.

6. Generic consent versus explicit consent

The survey shows that consent is usually obtained via generic consent. Consent is incorporated in the general terms of conditions or occurs via predefined browser settings. Most browsers accept cookies by default. In that case, users do not explicitly give their consent. The results from the focus groups show that most consumers are unfamiliar with the fact that browsers settings can be used to accept or block cookies and find it difficult to adjust browser settings to their preferences. The obligation for informed consent is therefore not being fulfilled adequately. Furthermore, the browser option for consent also need to be in accordance with the Dutch data protection act.

7. No distinction between cookies and spyware/malware

The ePrivacy Directive and the Dutch implementation in the telecommunication act both mention *information* that is stored or gained access to on users' terminal equipment, but do not define or distinguish between the nature of that information. In principle, no distinction is made between cookies and other types of data such as spyware and malware. Overlap is also possible: a cookie – or its effect – can in some cases be considered similar or equal to spyware or malware. The regulation regarding spyware and malware requires, until now, a very clear consent. If browser settings are allowed to serve as an alternative for informed consent, this may imply that even for spyware and malware consent via browser settings will be sufficient (or that cookies with spyware or malware characteristics will fall under a browser regime as well). This may have substantial effects for the risks for users, but also for supervision and enforcement.