Cookies Under Control

On June 5, 2012 the new Dutch legislation on the use of cookies enters into force. What does this mean for the online marketing business?

CONTENTS

By **Christiaan Alberdingk**
Thijm & Vita Zwaan

SOLV Advocaten
Schippersgracht 1-3
1011 TR Amsterdam

P.O. Box 755 38
1070 AM Amsterdam

W www.solv.nl

F +31 (0)20 530 01 70

E thijm@solv.nl
T +31 (0)20 530 01 75
nl.linkedin.com/in/cthijm
twitter.com/cthijm

E zwaan@solv.nl
T +31 (0)20 530 01 79
http://www.linkedin.com/in/vitazwaan
twitter.com/vitazwaan

NEW RULES FOR THE USE OF COOKIES

The online advertising market is increasing every year. The success of behavioral targeting is apparent. Advertisers, publishers and consumers are benefiting. But there's a catch.

The practice of behavioral targeting is to a large extent still a "wild west". Data on the search and browsing behavioral of consumers is gathered on a massive scale, used and sold to third parties, without the internet users having any knowledge of this conduct. Internationally there is a growing resistance against this practice.

When people's behavior is to a more or lesser extent being monitored, analyzed and contained, privacy is a concern. This concern was until recently not sufficiently addressed by the industry. The lack of transparency led to a growing distrust by politicians, lawmakers, consumer organizations and internet users. The European legislator introduced new, stricter legislation with regard to behavioral targeting and the use of cookies. This legislation is laid down in the amended ePrivacy Directive of 25 November 2009.

On 8 May 2012 Dutch Parliament adopted a Bill to amend the Dutch Telecommunications Act (Telecommunicatiewet, hereinafter 'DTA'). The new regime for the use of cookies boils down to the requirement of informed consent based on an opt-in system:

- Prior to installing or reading cookies on the terminal equipment of the end user, the end user should be informed, and consent of the end user should be obtained.
- If the cookies are used to collect, combine or analyze information on the use of different services of the information society by the end user for commercial, charitable or non-profit purposes, this is presumed to be a procession of personal data. That means the Dutch Data Protection Act is applicable.
- Functional cookies are exempted.

WHO SHOULD CARE

The new cookie rules affects the complete online marketing business since it is aimed at one of the essential elements of online advertising and behavioral targeting. In particular the following stakeholders should pay attention to the new legislation:

- Ad network providers;
- Publishers;
- Advertisers;
- Developers of digital media and ad serving technology;
- Affiliates and affiliate networks;
- Data providers;
- Online ad traders;
- Media agencies.

CONSEQUENCES

PRINCIPAL RULE: PRIOR INFORMED CONSENT

- **Technology**

The new legislation doesn't specifically apply to cookies. It applies to any technology

- by which information is stored on the terminal equipment of a user, or
- by which information already stored is being accessed.

It concerns not only personal computers, but also mobile phones and other mobile devices. Potentially, the legislation may even apply to televisions.

- **Information**

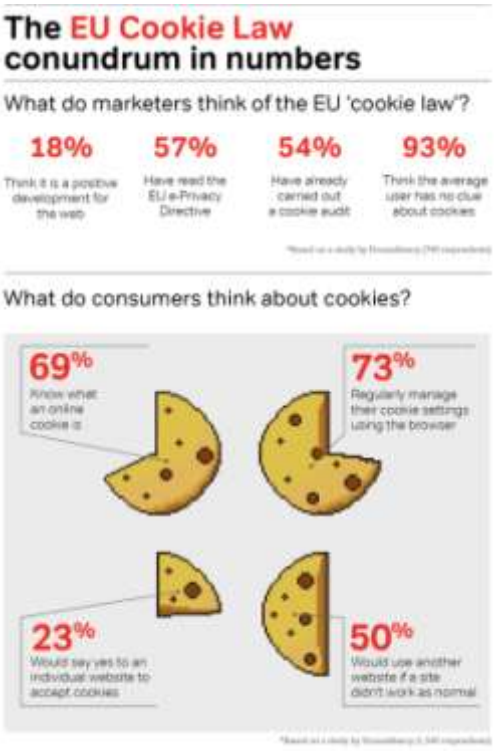
The information that has to be provided *prior* to placing or reading the cookie, needs to be 'clear and comprehensive'. It needs to inform the end user of the purpose of the cookie and the further processing of the data collected by the cookie.
This means that the end user should at least be provided with the following information:

- the fact that the cookie is being stored on the terminal equipment;
- the purpose of the cookie;
- the period it remains active;
- if the cookie is being used to track online behaviour for targeted advertising this should be mentioned too, including with whom the information is being shared.

The information has to be easily accessible and understandable to the users.

CONSEQUENCES

Image 1: Solv. Advocaten # June 2012



Source: Econsultancy.com

- **Consent**

There has been a lot of debate about the question how consent can be obtained. The legal requirement is that consent has to be *free, specific* and *informed*. In the preamble of the ePrivacy Directive it is made clear that browser settings may possibly be an adequate means of giving consent. Dutch government has confirmed that the present browsers are insufficient, mainly because they are set to accept cookies by default.

The explanatory notes to the adopted Dutch amendment state that consent has to be 'unambiguous'. This would be a stricter requirement than laid down in the ePrivacy Directive. However, Dutch government confirms that there is in principle no need for unambiguous consent. Clearly this contradiction in the process of legislation leads to insecurity and interpretation issues. The ePrivacy Directive concerns full harmonisation and not minimal harmonisation. An interpretation that leads to the requirement of unambiguous consent *per se* may therefore be in violation of the directive.

Consent can be revoked at all times by the user and the user should be informed of this possibility.

CONSEQUENCES

DUTCH DATA PROTECTION ACT

The requirement of obtaining informed consent before placing or further accessing cookies is in line with the ePrivacy Directive.

However, the adopted Dutch Bill goes considerably further and introduces an additional legal regime for the use of cookies. Any cookie used to collect, combine or analyze information of the user with regard to his online surfing behaviour, is presumed to involve personal data. As a consequence, the Dutch Data Protection Act is applicable to many different cookies, entailing an even stricter legal regime to the use of cookies. This part of the legislation will enter into force in January 2013.

It is important to note that the Dutch Data Protection Act holds further requirements than the cookie legislation laid down in the ePrivacy Directive, such as:

- the obligation to notify the processing of data with the Dutch Data Protection Authority;
- obligations with respect to security measures;
- the obligation to enable the end users to check and correct the processed data;
- if the data is being processed by a third party, the obligation to enter into a data processing agreement with this party;
- the processing of the data has to be based on one of the six statutory grounds, one of which is ‘unambiguous consent’.

Since it concerns a legal *presumption*, this may be refuted with evidence showing that no personal data are collected. In practise this will probably be difficult, and in any case it lays down the burden of proof at the user of the cookie.

This considerable aggravation of the requirements under the ePrivacy Directive has no equal in other Member States, placing the Netherlands in an exceptional position.

WHAT SHOULD STAKEHOLDERS DO?

- Contact the regulatory authorities about your concerns. The Bill leads to serious problems in terms of practical execution. These authorities still have to adopt policies on compliancy and enforcement.
- Join the self-regulation initiative of the Internet Advertising Bureau (IAB Europe and IAB Netherlands) and the European Advertising Standard Alliance (EASA), referred to as the Best Practice Recommendation on Online Behavioral Advertising. If you have joined already, keep working on further improvement so that the regulatory authorities will finally approve of it as a means of compliancy.

Take the following actions:

- Make sure you have a clear, informative and easily accessible privacy statement;
- Use preferably a pop-up screen with information about cookies and a tick-box to obtain consent;
- As a precaution: a notification of the data processing at the Dutch Data Protection Authority;
- Advertisers, publishers and ad network providers should work together in order to make sure that internet users are well informed about the use of cookies and to find ways to obtain consent in a centralized way;
- Make sure you have proper contracts with the parties you do business with. If collected data is shared with, sold to, or bought from third parties, make a clear agreement on, inter alia, security of the data, for which purposes the data will be used, who is responsible for which obligations under the applicable rules (cookies, privacy, data protection), warranties, indemnifications and liability.

5 FAQ'S IN BOX

1 TO WHICH TECHNOLOGY AND COOKIES DO THE NEW RULES APPLY?

First of all, the new rules *do not* apply to so-called functional cookies.

Examples are cookies that are stored and read to remember the personal settings and preferences of a user, such as the preferred language, cookies used for the processing of online orders and the execution of transactions.

The new rules *do* apply to any other cookies, flash-cookies, Java-scripts, web taps and spyware or similar software such as dialer programmes. Device fingerprinting and digital television are also covered.

The Bill makes no distinctions between first party or third party cookies.

Cookies used for website optimisation or analytics such as Google Analytics, are governed by the new rules. Most likely these even fall within the scope of the stricter regime in which it is presumed that personal data are processed.

2 WHO IS RESPONSIBLE?

Any party that places cookies on the terminal equipment of the user or accesses information already stored on this equipment should comply with the new rules. The regulatory authorities have stressed that there can be a shared responsibility, imposing at least some responsibly for the publishers.

The Bill is applicable to anyone who wants to store information or access information already stored on the terminal equipment of internet users in the Netherlands. Thus, also companies established outside the Netherlands are governed by the Bill.

3 HOW TO COMPLY?

The question of how to practically comply with the rules is essential, but has not been answered by the legislator. The responsible Ministers have given some guidance, however, the explanatory notes to the adopted amendment cause confusion. This much is clear:

The information that needs to be provided prior to placing the cookies has to be easily accessible and understandable to the users. This implies that a clearly visible link to the information most likely does suffice, however, a privacy policy as sole source of information is insufficient.

The consent of the user must be a clear indication of his wishes. A pop-up screen with clear and comprehensive information and a tick-box stating “I accept” seems at present the only way to comply with the new cookie rules.

The regulatory authorities have expressed that consent is not required for each individual cookie. Once the user has agreed to cookies of a specific ad network provider, this ad network provider doesn’t need to obtain additional consent for cookies serving the same purpose.

Users should always be given to possibility to opt-out.

4 WHAT ABOUT SELF-REGULATION?

The industry has adopted self-regulation in the form of Best Practice Recommendations. It entails a do-not-track register which the user can access via **www.youronlinechoices.eu**.

Although the regulatory authorities welcome this initiative as an improvement, it does not meet the requirement to obtain informed consent (yet). It entails an opt-out mechanism, and the way in which the information is provided is deemed as insufficient.

Eurocommissionar Neelie Kroes has more than once spoken in favour of self-regulation. Kroes expressed that if the industry is capable of implementing a well functioning do-not-track standard which creates transparency and is well enforced, such self-regulation is in compliance with the new cookie legislation. She announced to evaluate the progress of self-regulation mid 2012.

5 WHO WILL ENFORCE?

The new cookie rules are laid down in the Dutch Telecommunication Act. The Dutch Independent Mail and Telecommunication Authority (‘OPTA’) is the competent authority with respect to the enforcement of this Act. However, when personal data are involved, the Dutch Data Protection Authority (‘CBP’) is competent as well. The CBP has taken a strict position with regard to the compliancy questions, and especially when it concerns the information and consent obligations.

OPTA has recently expressed that it will enforce the new rules, focussing on the fields in which threats to the consumers are the largest.

OPTA is competent to give (high) penalties in case of non-compliance with obligations under the Dutch Telecommunication Act. The CBP can only impose an order with incremental penalties (*dwangsommen*). Following pending changes of the Data Protection Directive, the CBP may obtain power to also impose penalties in case of non-compliance.

With regard to cross-border enforcement, there are a few European bodies in which the regulatory authorities of the Member States work together.