Online tracking: to collect or not to collect, that's the question...

By Jacob Kohnstamm, October 2012

Few of us can imagine a life without our computer, smartphone or tablet. These wonderful devices have made our lives much easier and made many things possible. We can book our holidays from our own living room and stay in touch with friends and family from around the world. At the same time, we are being watched over our shoulder while surfing the Internet. It is possible for companies to track each and every move we make on the Internet at all times. The question is: should our every move be registered and our next moves predicted, just because technology allows for it? I beg to differ.

My expectations were therefore high when a technological answer to this dilemma presented itself in the form of a Do Not Track standard, to be developed by the World Wide Web Consortium (W3C). This standard was said to allow people to simply say yes or no to tracking. But my hope for such a simple and effective solution is rapidly fading.

Politicians, legal experts, companies and supervisory authorities on both sides of the Atlantic are currently engaged in an ongoing debate on the use of cookies and other technologies that collect information on people's behaviour on the internet over time. The information collected can be used to build detailed profiles of people in order to show them personalised advertisements.

While personalisation of services and advertisements might actually positively influence our experience of the Internet, there is no such thing as a free lunch. These so-called "free" services come at a price; in many cases you are not the customer, but actually the product of the service.

Because of a total lack of transparency by companies and a lack of awareness of individuals about these tracking activities on the Internet, our privacy is at risk. But how can we make informed choices if we do not even know that our privacy is at risk?

Not knowing does not equal not caring. User surveys have shown that more than 85% of the Internet users do not want advertising based on tracking and certainly would not consent to such practices. A large majority feels uncomfortable about it and therefore expects legislators or supervisory authorities to take action.

Furthermore, many studies show that the average person has great difficulties in finding, let alone deleting, tracking cookies on their device.

In response to this widely shared sense of creepiness amongst Internet users, the advertising industry in the USA and in the European Union have reluctantly started to offer options to opt-out from getting personalised advertisements.

In 2009 the European Union legislator revised the e-Privacy Directive, also known as the cookie law. The cookie law is applicable to all companies that place cookies on devices of

European citizens regardless of where these companies are based. Since, the European Data Protection Authorities have often provided detailed public advice on the implementation.

The legislation provides that a company may only place or read a tracking cookie on a user's device if the user has given his or her consent, after having been provided with clear and comprehensive information.

Naturally, cookies that are placed for the sole purpose of carrying out the transmission of a communication and those that are strictly necessary to provide the requested service, are excluded from this consent requirement.

But for all cookies placed for any other purpose, the user should consent before a company starts collecting data about the user's Internet behaviour.

According to the EU legislation, using the web browser to obtain consent is also an option, as long as it is technically possible, effective and in accordance with all the requirements for consent to be valid. Users cannot be deemed to have consented simply because they use a browser or other application that by default enables tracking.

To ensure consent is valid, the browser must therefore by default reject tracking cookies and require the user to explicitly indicate to accept tracking cookies.

This means that clear and understandable information must be provided after which the user can consent to being tracked by opting-in. Merely providing an opt-out possibility to users is therefore clearly not sufficient.

According to European laws Do Not Track should be "do not collect". It seems however that Do Not Track in the USA may be limited to "do not target" and this greatly concerns me, since the European law also applies to companies outside of Europe as well. Whenever a cookie is set on a device of a European citizen, the company should comply with the cookie-requirements.

As mentioned before I had high expectations of the initiative of W3C to develop a worldwide Do Not Track standard, as its aim was to create a mechanism by which users could indicate their tracking preferences in a simple and persistent manner. Thereby enhancing user control and improving online privacy.

My high expectations were shared by the White House, the US Department of Commerce (DoC), the US Federal Trade Commission (FTC) and the European Commission. We all welcomed the idea of a technical solution that would deliver transparency and ensure legal compliance on both sides of the Atlantic.

However, it seems the discussions have been hijacked by commercial interests. After intensive deliberations between the members of the W3C Working Group, proposals have been put on the table that, instead of providing users with a clear yes-or-no-choice, allow the advertising industry to collect our each and every mouseclick, without informing us and even without asking our consent. If adopted this way, the Do Not Track standard would be

utterly deceptive to users and act as a disguise for a continuation of unfair and intransparent business practices.

Considering the W3C's aim to develop worldwide standards involving all different stakeholders, any result from W3C will only make sense if it also leads to compliance with EU law. Unfortunately we are now facing a situation in which companies invest in a mechanism that does not lead to compliance with European requirements.

The time for the industry to act responsibly is ticking away. It is no longer five to twelve, but way past midnight. When it comes to large scale infringements of European privacy legislation, supervisory authorities are left with no other choice than to enforce.

Jacob Kohnstamm is Chairman of the Dutch Data Protection Authority and the Article 29 Data Protection Working Party. The Article 29 Data Protection Working Party consists of all European Data Protection Authorities. It has an advisory status and acts independently.