Public Lecture, University of Edinburgh, School of Law

Edinburgh, 7 July 2011

"Do not track or right on track? – The privacy implications of online behavioural advertising"

Peter Hustinx

European Data Protection Supervisor

Ladies and gentlemen,

First of all, I want to thank the University of Edinburgh, School of Law, for the invitation to give this lecture in the context of a larger conference on the same subject.

Although I have accepted this invitation with pleasure, I must confess that this arrangement also created a sense of embarrassment, particularly because I was unable to attend today's sessions. So, how could I do justice to today's speakers and avoid the risk of an undue overlap or perhaps even an overdose of privacy and OBA?

I have decided to build on the strengths of this arrangement and assume that you are all now familiar with at least the main lines of interest based advertising, and the technology of user choices and user control. My short definition of OBA is that it is the presentation of targeted advertising on websites based on large scale tracking of consumer behaviour online.

There are different ways to do this, but it typically takes ad network providers as an active link between website operators and advertisers. It also involves the storing of cookies on the user's computer and browser settings in a mode to accept those cookies. Other methods may be even more invasive, such as 'deep packet inspection' by internet service providers, but that should perhaps be left for another occasion.

The internet advertising industry has been developing over the last 15 years. It has contributed to a lot of free content on the internet. In fact, free content is now the standard on the net. However, nothing is really free and this content is made possible by systematic tracking and tracing of consumer behaviour online and the considerable value this apparently generates. At present, OBA involving monitoring across websites accounts for a limited percentage of this activity, but it is growing fast. The interests represented here are to a large extent legitimate, but that is not decisive.

Historic context

Before 1995, advertising was mostly newspapers, radio and television, typically broadcast and not so targeted. The public was free to select relevant information without being observed or monitored. Consequently, there was no risk of restriction or chilling effect on the freedom of information. That is different now. The fact that the government is not directly involved in the monitoring does not make it less problematic.

Before 1995, the confidentiality of communications was a widely practiced rule. Interception or monitoring of communication was only allowed under strict conditions, subject to a series of safeguards. Consequently, there was no risk of a chilling effect on the free communication of citizens. Nowadays, communications over the internet are often systematically monitored and most users of free services are not aware that they have implicitly accepted this.

Before 1995, the private life and personal data of citizens was also better protected than it is now. The risk of systematic tracking of consumer behaviour online and the building of extensive profiles have changed this situation. The risk of further use of these profiles outside the context of online advertising only underscores the problem.

So, there are some important ups and downs. Some refer to a paradigm shift. One might also speak of an erosion of fundamental rights and a market failure, as certain public interests have apparently not been sufficiently included in the way the internet has developed so far. It seems in need of some correction, be it by law, by self-regulation or by technology.

This is all the more evident, if we imagine how this situation could develop in the near future. Personalisation seems innocent, but may be close to unfair discrimination of consumers who

no longer operate in a transparent market. Or from a different angle: different public interests, including law enforcement, could easily develop into "free riders" on the waves of internet profiling.

Need for a better balance

So, there is little doubt that a better balance is needed. It may be useful to see how the current legal framework can help to find that better balance.

Speaking of balance, it is also clear to me that the protection of user's privacy should be done in a user friendly manner. Even the most radical user would probably not like to see the good sides of the present internet entirely disappear in the process!

At a general level, there also seems to be a growing consensus that a better balance can be found on the basis of three key principles: i.e. transparency, fairness and user control.

These principles are also of crucial importance in the present legal framework that provides two keys to online privacy. The first key is triggered by the "processing of personal data" and laid down in Directive 95/46/EC ("Data Protection Directive") that is currently subject of a review to make it more effective. The second key in Article 5(3) of Directive 2002/58/EC ("e-Privacy Directive") is triggered by the "storing or accessing of information stored in the user's terminal". It was revised in 2009 and is currently subject of implementation into the national law of the Member States.

Let me start with the second key and come back to the first key at a later stage. Let me only say now that the scope of the Data Protection Directive and the concept of "personal data" are often underestimated. As to Article 5(3) of the e-Privacy Directive, it is important to know that the storing of information and the accessing of information stored in the user's terminal are considered as an intrusion in the private sphere of the user. This is expressly stated in recital 24 of the 2002 version of the Directive and recital 65 of the revised version.

It is also part of a remarkable history. Its previous version started off as a "right to consent" and was adopted in 2002 as a "right to refuse" after heavy lobbying of the internet industry. In the light of experience, this was again after heavy lobbing, turned into a "right to consent" in 2009, and the discussion on the subject has still not fully settled.

Article 5(3) of the e-Privacy Directive is based on a distinction of three different scenarios. The first one is where the storing of information is considered as legitimate. This is the case where it only takes place for the transmission of an electronic communication or where it is necessary to provide a service requested by the user. This is typically the case for 'session cookies'.

In the second scenario, the storing of information is only allowed, if certain conditions have been fulfilled. This is the case for different kinds of online advertising.

In the third scenario, the storing of information is considered unlawful. This covers malware, spyware and similar devices.

Further analysis

As to the second scenario, a careful analysis of the old and new version of Article 5(3) can only lead to the result that a provision on the "right to refuse after clear and comprehensive information" has been replaced by one according to which the same activity is only allowed on condition that the user concerned has given his or her consent, having been provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing.

There is no doubt that this clear language will be considered as a "right to consent" in spite of the confusing and somewhat contradictory text of recital 66 in the 2009 version, which both refers to a right to refuse and a right to consent. The case law of the European Court of Justice is crystal clear on such situations.

The new text of Article 5(3) requires consent of the user concerned, which must be given before the storing or accessing of information. The e-Privacy Directive also makes it clear that this consent should fulfil the requirements of Article 2(h) of the Data Protection Directive, i.e. it should be a "freely given, specific and informed indication of his wishes" by which the user signifies his agreement to information being stored or accessed on his terminal.

The only points on which the new text is open are the scope and the means of consent. Indeed, recital 17 of the e-Privacy Directive has made it clear that consent may be given by "any

appropriate method enabling a freely given specific and informed indication of the user's wishes". This is very welcome, as we will see, to find an appropriate solution in practice.

The information given should be "clear and comprehensive". This means that it should be clear, precise and easily understandable, and should cover all relevant substance. It follows immediately from the text that the information should be given before the user's consent. This information should also be readily available to the user without great efforts: the user must be provided with the relevant information.

The text does not specify who should provide this information. However, it is obvious that the first candidate to do so is the ad network provider who stores or accesses information on the computer terminal. This does not prevent that the website operator or publisher is often also in a good - or perhaps even better - position to provide the required information.

The frequency of the information is not mentioned. The text certainly does not require that the information is given each time a cookie is stored or accessed on a terminal. Indeed, it allows a practical approach under which both information and consent are provided at certain intervals and for certain categories of activities.

This approach has already been suggested in the Article 29 Working Party's Opinion of June 2010 (WP 171). This opinion has been largely misunderstood by the advertising community and perhaps also by other relevant actors. Its intention was not only to clarify the meaning of the new legal framework, but also to show an area for further development in practice. It was designed as a challenge for industry at a time where discussion and creative development were still largely possible.

Browser settings

This leads to a few other issues, such as the role of browser settings. Recital 66 of the revised e-Privacy Directive is often referred to in this context. However, what it says is 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." As most current browsers accept cookies by default and most current users lack the skills to change browser settings, this recital refers to a scenario that is presently too often not realistic. However, this could of course change in the future.

Another question that is sometimes raised is whether the new text of Article 5(3) is based on "opt-in" or "opt-out". Although some would rather avoid the term "opt-in" or "prior opt-in", it is not so difficult to see that this is exactly what the present text requires. The assumption that this "opt-in" should be exercised each time a cookie is stored or accessed, has led to a kind of tunnel vision on the subject. Indeed, a solution should be user friendly *and* effective.

Although the revised Directive should have been implemented into national law by 25 May 2011, only a small minority of Member States have actually managed to do so. Those that have implemented Article 5(3) have mostly followed the analysis presented here.

That in any case applies to Denmark as the first relevant example. The UK has provided for a soft landing, but it also follows the consent model. The Dutch implementation - which is now before the Senate - also follows that model in a version close to the Directive. However, it also specifies that systematic monitoring of the user's behaviour should be considered as "processing of personal data" under the Data Protection Directive.

Innovative developments

Since Article 5(3) was adopted, some innovative developments have taken place. Browser providers – such as Microsoft, Mozilla and Google – have developed their own favourite solutions. However, all of them are based on an opt-out model. Self-regulation has also been developed more actively. This applies to initiatives by NAI in the US and by EASA and IAB Europe on this side of the ocean. However, typically these initiatives are designed to facilitate an opt-out model, and thus fit better with the previous model than with the current one.

In a speech delivered in September 2010, the Commission's Vice-President Neelie Kroes, responsible for the EU Digital Agenda, has encouraged the advertising community to develop a self-regulatory framework in compliance with the e-Privacy Directive.

In a speech delivered on 22 June 2011, she welcomed the recent adoption of a Best Practice Recommendation and Framework on behavioural advertising by EASA and IAB Europe. However, these associations have in fact failed to implement the new consent requirement. At the same time, she expressed support for a US driven 'do-not-track' initiative that – although

valuable – also seems to fall short of the e-Privacy Directive requirements. Unfortunately, this also raises doubts on the position of the European Commission on this subject.

This is why I want to call on the Commission to ensure that Article 5(3) of the e-Privacy Directive is fully respected. Systematic tracking and tracing of consumer behaviour online is a highly intrusive practice and now rightly subject to more stringent requirements. Although initiatives for increased transparency and consumer control in the online environment are most welcome, this should not result in a limitation of consumer rights. The Commission should avoid any ambiguity as to its determination in making sure that these rights are delivered in the European Union.

More transparency, fairness and user control in line with Article 5(3) of the current Directive would require the inclusion of a "privacy wizard" in each browser so as to ensure that every user has been able to express his or her own preferences. Ideally, this should be combined with a "privacy-by-default" setting according to which third party cookies are rejected, unless the user decides otherwise.

In practice, solutions at either side of the Atlantic may come so close to each other as to become virtually identical. However, this requires more time for further discussion and development, and above all, the willingness to come to a workable outcome in line with the Directive.

Personal data

At this point, let me come back to the other key to online privacy: the applicability of the Data Protection Directive. This depends on the processing of "personal data", i.e. any information relating to an identified or identifiable natural person.

This is the case for OBA, as it typically leads to the collection and further processing of information about personal characteristics that is used to target and "single out" individuals. In fact, the closer persons are targeted, the more likely this will result in the processing of personal data. The Dutch implementation of Article 5(3) clearly builds on this interpretation.

The Data Protection Directive applies where such processing is taking place in the context of the activities of an establishment of the controller in the European Union, or uses means that

are located in the EU. It is likely that the latter criterion will be replaced by targeting persons in the EU or providing a service on the European market.

This would lead to an interesting interaction of the "two keys to online privacy". The Data Protection Directive applies, and consent as required by Article 5(3) may also be relevant for further processing, if its quality and scope are adequate. All other requirements under the Data Protection Directive – such as limited retention, use of data for compatible purposes and rights of data subject – will also have to be respected. Cooperation of supervisory authorities will be necessary, both in the EU and internationally.

Let me finally mention a few other perspectives in the context of the current review of the EU legal framework for data protection. The impact of the Lisbon Treaty is likely to lead to a more comprehensive approach across all EU policy areas. There is also a strong emphasis on greater effectiveness in the light of technological change and globalisation, and reduction of unhelpful diversity and complexity in the EU.

This will probably lead to more responsibility and accountability of controllers, stronger rights for data subjects and more enforcement powers for supervisory authorities. All these elements are also relevant for OBA and online privacy in general.

I very much hope that the European Commission will come up with ambitious proposals later this year, probably in November.

In the US, there are also interesting developments that are different, but seem to go in a similar direction. More global privacy will require more compatibility and interoperability of our legal approaches, especially for the online environment. Today’s subject may turn out to be an interesting test case for our determination and creativity to provide privacy online.

Thank you very much for your attention.