

Online targeted advertising

This document is a partial, unofficial and uncertified translation of the report presented by Mr Peyrat, Commissioner, to the French Data Protection Authority (CNIL) on February 5, 2009 and released on March 26, 2009:*

http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/Publicite_Ciblee_rapport_VD.pdf

The translated sections address the recent evolution in the industry organization, potential threats, as well as legal issues raised by online targeted advertising and the CNIL current views on these issues (anonymous data, applicable law, notice, objection right).

The other sections describe in an educational manner existing technologies, processes and business models.

**Document drafted by Pascale Gelly and Elisabeth Quillatre – Cabinet Gelly*

Translation of table of content

I. Presentation

- A. The fuel of the e-economy
- B. Types of online advertising
- C. Organization of the online advertising models

II. Tracking Technologies

- A. Publishing of online advertising by advertising agencies
- B. Capability to collect data
- C. Capability to track the Internet user

III. Profiling

- A. Predictive profiles
- B. Explicit profiles
- C. Anonymity of collected data?

IV. Panorama of Online Advertising Models

- A. Amazon: onsite behavioural advertising
- B. Google: the champion of the contextual model
- C. Facebook: on site personalized advertising
- D. Linked-in: personalized advertising in network
- E. Tacoda/AOL: behavioural advertising in network
- F. Phorm: behavioural advertising by telecom operator

V. Tendencies and Prospective

- A. A Concentration of stakeholders of the online advertising sector
- B. A convergence between advertising provider and content provider
- C. An extension of fields of application
- D. An increasingly precise use of geo-location

VI. Threats

- A. Risk of “monetization” of profiles
- B. Risks linked to the creation of mines of personal or sensitive data
- C. A risk for user trust
- D. The generalization of an imperfect opt-out approach
- E. An inefficient management of cookies

VII. Challenges for Data Protection Authorities

- A. The applicability of legislation on the protection of personal data
- B. Promoting a better information of Internet users
 - 1. Obligation to inform bearing upon online advertising stakeholders
 - 2. Information of the public on the means to control their traces
- C. Promoting products and services respectful of personal data protection
 - 1. The quality-label advantage
 - 2. Promoting standards compliant with personal data protection

VIII. Conclusion

V. Tendencies and Prospective

A. A Concentration of stakeholders of the online advertising sector

There has been recently a concentration of online advertising stakeholders: merger of TACODA with AOL's advertising agency, acquisition of the network RightMedia by Yahoo (for 680 million dollars) or even acquisition of Aquantive by Microsoft (for 6 billion dollars). But the current main stakeholder in online advertising is undoubtedly Google, which recently acquired the advertising network DoubleClick (for 3.1 billion dollars), and has advertising distribution agreements with the search engines AOL, Yahoo or even Ask.com. In the United States, estimations point out that Google currently distributes almost 70% of online advertisements¹.

The trend toward the merger of online advertising networks is therefore strong, and implies an expansion of these networks' capacities to monitor and collect data related to Internet users.

B. A convergence between advertising provider and content provider

The functions of online advertising provider and online content provider have for a long time been relatively distinct. Content providers held specific personal information related to their customers, while advertising networks rather owned anonymous information predictably based on the observed behavior of Internet users.

With their recent acquisitions, the digital world leaders Google, Yahoo and Microsoft end up with the dual role of content and advertising providers. These stakeholders have, in theory, the unique ability to know a lot of information on Internet users both through what Internet users voluntarily provided to them and by observations they can obtain about their behavior.

This convergence is not a coincidence but effectively enables the main content providers to better define and control ads provided to Internet users and thus their chain of income.

Several questions arise for these stakeholders who wear two hats:

- What personal information are used to carry out targeted advertising?
- What personal information are transferred to third parties, and especially to advertisers?
- What border exists nowadays between personal data collected in order to provide a service and data collected in order to provide targeted advertising?
- Is the border between personal data collected in order to provide a service and data collected in order to provide targeted advertising likely to evolve in the future?

¹ In July 2008, adding the number of searches conducted by Google (61.9%) with its two affiliated companies, Ask (4.3%) and AOL (4.1%), it is showed that 70.3% of the queries have included Google ads (see <http://www.comscore.com/press/release.asp?press=2405>). In addition, according to other estimates, almost 70% of ads, apart from search engines, are displayed by Google and DoubleClick (see <http://www.attributor.com/blog/get-your-fair-share-of-the-ad-network-pie/>). Other estimates, more conservative, place Google around 50%, which remains sizeable.

C. An extension of fields of application

If the collection of data related to Internet users is nowadays primarily limited to the analysis of behavior on the web, changes can be contemplated:

- Targeted advertising projects for IPTV over broadband are nowadays being developed² enabling for example to replace the traditional advertising screens by ads targeted according to the household watching it,
- Communication media such as Internet, Telephone and Television are converging towards a common technology, namely IP, provided by the same operator (the “triple” or “quadruple play”),
- IT capabilities to analyse and to store data are constantly growing³.

One could imagine that TV commercials will soon be adapted to the profile of the Internet user, or conversely that the ads proposed on the Internet will be related to the analysis of television content viewed by the Internet user. It does not seem impossible neither to imagine that companies provide ads based on keywords found in a telephone conversation over IP.

In this spirit, **the example of Phorm, previously described, allows to speculate on the future enhanced role of telecommunications operators in the world of behavioural advertising.**

D. An increasingly precise use of geo-location

A lot of online advertising systems provide a “geo-located” content assumed from the IP address of the Internet user.

This geo-location is quite rough as it is limited at best to a city or a region.

However new geo-location tools, much more precise, are appearing in the world of targeted advertising.

Indeed, current mobile terminals often offer embedded GPS which can provide very precise geo-location information. The organisation W3C responsible for the definition of Web protocols has recently defined a standard⁴ enabling web browsers to access and to operate geo-location information given by any means (e.g. IP address, RFID, WiFi, Bluetooth, GSM, GPS) in particular to identify the centers of interest of a person, to annotate a content with location information, to position a user on a map, to send alerts when the points of interest are in the vicinity of a person, to obtain updated local news or even to insert geo-located status information in social networks. Browsers could then potentially transfer these data to service providers.

In parallel, **Google has developed a system of geo-location based on the detection of the**

² The company PacketVision has in particular made a presentation of such a device before the CNIL in January 2008.

³ These analysis capabilities will be less and less limited to text, and will also cover sound and image.

⁴ See <http://dev.w3.org/geo/api/spec-source.html>

nearest WiFi terminals or on the relay antenna to which a mobile is connected. The system detects the closest antenna to the Internet user and then queries⁵ Google to translate this information into precise geo-location information within a few hundred meters.

These tools enable to anticipate ads targeted as close as possible to the Internet user.

⁵ Indeed, individuals and professionals who use wireless networks emit signals which can be distinguished in particular by identifying the MAC address of their equipment. Google has thus covered the areas of many cities to build a large database to link each wireless terminal with a specific geographical address.

VI. Threats

A. Risk of “monetization” of profiles

The stakeholders benefiting from online advertising are:

- 1) Providers:
 - a. of targeted advertising (on site or on network)
 - b. of content or services which display ads against payment.
- 2) Advertisers wishing to sell their products and boasting them through ads.

As seen earlier, the border between content providers and advertising providers tends to disappear at Google, Yahoo, Microsoft or AOL. Therefore, these “providers” have both personal data explicitly provided by the Internet user and data collected through monitoring his behaviour.

If nowadays, the transfer of personal data between “suppliers” of content or ads and advertisers are non-existent or limited, nothing indicates that this border will not be crossed one day. This risk could have important consequences which must be taken into account for at least two reasons:

- 1) The state of current technology enables all stakeholders to exchange information easily and without control by the Internet user. When an Internet user clicks on an ad displayed by an advertising supplier, no technological barrier is preventing the advertising provider to transfer information related to this Internet user to the advertiser (example: gender, age, last visited pages, keywords, etc.). Already, if the advertiser has built an ad according to very specific criteria and if an Internet user “clicks” on it, the advertiser will assume that the Internet user meets certain characteristics associated with the profile concerned.
- 2) Providers of advertising or content are tempted to monetize some of the information they hold on Internet users to advertisers. The advertiser may already select his clients based on a risk (by age, location, estimated income, etc.) or could propose a rate “according to the consumer’s looks”.

In theory, the Data Protection Law would regulate the exchange of data between an advertising (or content) provider and an advertiser. But what would happen if these exchanges do not involve personal data? Can they be general data corresponding to the “anonymous” profile of the Internet user (e.g. age, gender, location). In this case, the supplier of advertising or content would probably use the argument of “anonymity” of created and transferred profiles to evade the constraints of the law.

The advertiser could meanwhile perform a “dis-anonymization” of the received data, by associating them with the collected data. It can also be contemplated that the advertiser acts upstream from the collection of personal data:

- a selection of customers he wishes to get through the received information,
- a price adjustment based on a perceived risk or an estimated income.

The consequences of the connivance between the content or advertising provider and the advertiser enables to envisage a number of significant risks to liberties, particularly in the following areas:

- **Credit and Insurance:** evaluation of the solvency or the health of the applicant without him being aware of it.
- **Recruitment site:** selection of persons receiving the recruitment offer based on sexual orientation, political opinions, health, etc.
- **Price:** price adjustment depending on the profile of the Internet user.

B. Risks linked to the creation of mines of personal or sensitive data

As the cost of storage of information is increasingly low⁶ and as Internet users increasingly produce data and trails, it is very tempting to collect a maximum of data related to Internet users even if the purpose of each data is not always defined at the time of collection. In parallel, the increasing calculating power and the constant sophistication of “data-mining” tools enable to foresee ever more advanced analysis of these data warehouses.

In case of serious flaw in the IT systems storing these data, a mine of information could be available to an ill-intended third party.

This risk is amplified when the collected elements include sensitive data (health data, political opinions, sexual orientation, etc.). This inclusion might be purely accidental, for example, if one collects the centres of interest of the Internet user among which could be a disease affecting him or his political opinions.

In its confidentiality charter, Yahoo expressly specifies that it takes measures in order to exclude sensitive data from the collection related to the profiling of Internet users, which proves that this is already an issue. The odds are that Microsoft and Google have similar guarantees, but what does really happen in practice? What about the stakeholders who are less-known or willing to distinguish themselves from the competition?

C. A risk for user trust

In a context of lack of transparency by content or services providers on profiling mechanisms and collected data, the Internet user may see these mechanisms as very intrusive. **In the future, the CNIL will certainly be called out by Internet users on this issue and should require clear information from online advertising stakeholders.**

D. The generalization of an imperfect opt-out approach

Several behavioural advertising⁷ systems provide an “opt-out” mechanism enabling not to

⁶ It can be noted that Google Mail offers a data storage free of charge for its users. In November 2008 this capacity was 7265 MB and is growing each day from 0.35 MB.

⁷ See especially the opt-out system of Google (http://www.google.com/privacy_ads.html) or Microsoft (<https://choice.live.com/advertisementchoice/Default.aspx>) and the one of TACODA previously mentioned.

receive targeted advertising. **Paradoxically, this “opt-out” often takes the shape of a cookie placed on the Internet user’s station.** If this “opt-out” cookie is found on the station of the Internet user then he will not receive targeted advertising.

The main targeted advertising stakeholders have joined the association “Network Advertising Initiative”, which offers a comprehensive tool⁸ in order to individually object to receiving ads on each network concerned, as shown in the abstract from the site below:

Opting out of an ad network program using the NAI Opt-out Tool should not affect other services provided by NAI members that rely on cookies, such as email or photo-hosting. [Click here for more information.](#)

If you have any questions, please visit our [FAQ section.](#)

Opt-Out Status

Network	Status	Opt-Out
aCerno More Information	No Cookie You have not opted out and you have no cookie from this network.	Opt-Out <input type="checkbox"/>
Advertising.com More Information	Active Cookie You have not opted out and you have an active cookie from this network.	Opt-Out <input type="checkbox"/>
Akamai More Information	Active Cookie You have not opted out and you have an active cookie from this network.	Opt-Out <input type="checkbox"/>
AlmondNet More Information	No Cookie You have not opted out and you have no cookie from this network.	Opt-Out <input type="checkbox"/>
Atlas More Information	Active Cookie You have not opted out and you have an active cookie from this network.	Opt-Out <input type="checkbox"/>
BlueKai More Information	No Cookie You have not opted out and you have no cookie from this network.	Opt-Out <input type="checkbox"/>

This “opt-out” by cookie approach is certainly a step forward, but it remains imperfect for several reasons:

- The Internet user is rarely informed or even aware of this possibility because the targeted advertising agencies are often “invisible” to him.
- The use of a cookie means that the Internet user has to systematically⁹ re- “opt-out” whenever he erases all of his cookies. It is a fact that more and more Internet users regularly delete cookies placed on their PC.
- The “opt-out” does not cover the collection of data, but only the distribution of targeted advertising. Internet users’ data continue to be collected by these targeted advertising networks (in order to make statistics).

Only an “opt-in” related to both the data collection and the display of behavioural advertising could actually give a real control to users. It is however unlikely that the industry follows this approach as it would greatly reduce the number of Internet users who can be traced and receive targeted advertising.

⁸ See the page http://networkadvertising.org/managing/opt_out.asp

⁹ TACODA has recently developed a partial parade to this issue by using a technical trick consisting to explore the “cache” memory of pages already visited by the Internet user in order to detect an “opt-out” even if he has erased the cookies.

Furthermore, in its new solution unveiled in March 2008, Google proposed to install a “plug-in” on the Internet browser enabling to perform an opt-out resistant to the deletion of cookies.

E. An inefficient management of cookies

Even if the management of “opt-out” is imperfect, theoretically the user has the opportunity to implement tools to better control the dissemination of his personal data.

Most major content providers publish a “Confidentiality Policy” specifying that cookies are for various purposes including advertising. These “Confidentiality Policies” also specify how the user may block or delete cookies, which may give the impression that the Internet user has a real choice.

In practice this choice is often illusory:

- **If the Internet user blocks all cookies, he would be prevented from using almost any service on the Internet nowadays¹⁰.**
- **If the Internet user chooses to individually authorize each cookie on a case by case basis, he will find himself with an endless number of confirmation messages which would quickly impede his navigation.**
- **Finally, the alternative of making a manual deletion of cookies at the end of each session is also almost impractical.**

Today these constraints entail that in reality most Internet users do not opt for a real control policy over cookies¹¹.

¹⁰ For instance, on the pages of its website dealing with cookies, Yahoo! Indicates to the Internet user how to block them, but also states that “If you choose to block all cookies, you will not be able to use Yahoo! products or services requiring the creation of a Yahoo! Account”.

see: <http://info.yahoo.com/privacy/fr/yahoo/cookies/>

¹¹ In this regard, we can still observe that the latest versions of browsers (i.e. Internet Explorer 8, Google Chrome etc.) enable to create browsing sessions at the end of which all cookies installed during the session are automatically deleted. This new approach is technically interesting but it is too early to know if it will be adopted by Internet users.

VII. Challenges for Data Protection Authorities

A. The applicability of legislation on the protection of personal data

The first question is about the applicability of personal data protection law. **In terms of online advertising, it may seem difficult at first glance to determine whether the implemented processing relates to personal data or whether the processing is anonymous.**

Besides, the means to inform the recipient of advertising should be addressed in the event that the legislation on data protection applies. **The respect of individuals' rights (prior information, right to access, right to rectify, right to object) is sometimes undermined in the field of online targeted advertising due to both technical and economical constraints.**

The European Directive 95/46/EC adopts a very broad definition of the concept of personal data¹².

In its opinion 4/2007 of June 20th, 2007, the WP29 provided guidance on how to interpret the concept of personal data according to the Directive 95/46/EC. The WP29 also reminded that the ultimate purpose of the rules contained in the directives on data protection¹³ is to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with regard to the processing of personal data.

According to this opinion, the definition of “personal data” is based on four elements, namely “any information”, “relating to”, “a natural person”, “identified or identifiable”. These elements are closely linked and interdependent, but together they determine the pieces of information to be considered as “personal data”.

The notions of “*relating to*” and “*identified or identifiable*” well deserve a thorough analysis.

The opinion states that “***In general terms, information can be considered to “relate” to an individual when it is about that individual***”. It was also noted that “*data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated*”.

According to this analysis, since the content of an ad is targeted according to a profile previously established, data protection legislation should apply. Data processed for online advertising clearly relate to the behaviour of an individual.

The opinion adds that “*It is sufficient if the individual may be treated differently from other persons as a result of the processing of such data*”. Such is the case in the scenarios presented in Part IV.

¹² It is “any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

¹³ Directive 95/46/EC on “data protection” and Directive 2002/58/EC on “privacy and electronic communications”.

The information should also refer to an “identified or identifiable” natural person. The WP29 states that *“while identification through the name is the most common occurrence in practice, a name may itself not be necessary in all cases to identify an individual. This may happen when other “identifiers” are used to single someone out. [...]. Also on the Web, web traffic surveillance tools make it easy to identify the behaviour of a machine and, behind the machine, that of its user. Thus, the individual’s personality is pieced together in order to attribute certain decisions to him or her. Without even enquiring about the name and address of the individual it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual’s contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense. In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her name”.*

This analysis shows that identifiers used in “tracking cookies” lead to a form of identification of an individual within the meaning of the WP29 interpretation.

The article 29 Working Party stated in its opinion on data protection issues related to search engines that *“When a cookie contains a unique user ID, this ID is clearly personal data. The use of persistent cookies or similar devices with a unique user ID allows tracking of users of a certain computer even when dynamic IP addresses are used¹⁴. The behavioural data that is generated through the use of these devices allows focusing even more on the personal characteristics of the individual concerned”.*

Therefore, it is possible to consider that the data elements included in profiles such as age, gender or location, are personal data in so far as they are linked to this identifier¹⁴.

Furthermore, it appears that most targeted advertising systems are based on the collection of IP addresses. The opinion clarifies that an IP address assigned to a user during its communication is a personal data¹⁵. In this context, if the ad is displayed by an advertising agency distinct from the website visited by the Internet user, the agency can generally be considered as “data controller”.

The CNIL itself has often pointed out that IP addresses are personal data, particularly during the review of the law on fight against terrorism, of the decrees [*secondary legislation*¹⁶] implementing the law on trust in the digital economy or of authorization requests filed by copyright agencies.

It follows from the foregoing that the legislation on data protection would have, to a large extent, vocation to apply to online targeted advertising. **Therefore, when online targeted advertising relies, for instance, on the tastes and behaviours that may be linked to an identified or identifiable individual, it must be carried out in accordance with data protection principles.**

¹⁴ Even if an identical cookie were assigned to several people in the same category, the classification of a person in his/her category generally involves a processing of personal data.

¹⁵ A recent decision of the Court of Appeal of Rennes on May 22, 2008 confirmed this analysis.

¹⁶ Added by translator

B. Promoting a better information of Internet users

1. Obligation to inform bearing upon online advertising stakeholders

One of the major challenges for online advertising is the quality of information provided to the concerned individuals. It is crucial that concerned individuals can be fully aware of the use of their data, whether data are provided on their own initiative (i.e. creation of explicit profile) or collected without interference from them (i.e. creation of predictive profile based, for instance, on purchase history, analysis of navigation and queries).

As of 2002¹⁷, the European legislator has been concerned with the issue of Internet users' information when connexion witnesses such as "cookies" are used by websites; establishing a principle of information and a right to object.

This provision has been implemented in French law at the revision of the Data Protection Act of 6 January 1978 which includes a specific provision on this issue.

Thus, the amended Act of 6 January 1978 states in its Article 32-II the obligations bearing upon websites publishers who use automated processes for collecting data such as "cookies".

The principle stated by law, thereby confirming the doctrine of the CNIL in this matter, is that of clear and comprehensive information of Internet users. The latter must be informed of the purpose of "cookies" and of the means to object to this process¹⁸.

The Law provides that this information requirement is not necessary if the "cookie":

- has for sole purpose to enable or facilitate electronic communication (i.e. ease of navigation during online registration and administrative formalities)
- or is strictly necessary for the provision of an online communication service at the express request of the user (i.e. creation of its "shopping basket" when ordering online).

As to whether Article 32-II should apply when the cookie enables the exchange of all types of data – personal or otherwise – between the IT device on which it is installed and the data controller's IT servers, the Commission opted for the following approach¹⁹.

It appears that Article 32-II is applicable only if the processes to access or enter information into the user's terminal equipment carry out a processing of personal data. This analysis has

¹⁷ Directive 2002/58/EC on "privacy and electronic communications", article 5.

¹⁸ [Added by the translator: Article 32-II: "*Any person who uses an electronic communication network shall be informed in a clear and complete manner by the data controller or his representative regarding:*
- *the purpose of any action intended to provide access, by means of an electronic transmission, to information stored in his connection terminal equipment, or to record information in his connection terminal equipment by the same means;*
- *the means he has to object to such action.*"]

These provisions shall not apply if the access to information stored in the terminal equipment of the user or the recording of information in the terminal equipment of the user is-
- *exclusively intended to allow or facilitate communication by electronic means; or*
- *strictly necessary for the provision of an online communication service at the user's express request"*]

¹⁹ The CNIL was interviewed in December 2005 by the *Forum des Droits sur l'Internet (FDI)* on this issue. The answer given by the Commission was taken into account in the FDI Recommendation on "adware and spyware" released on July 11, 2006.

for effect to exclude the application of the requirements of Article 32-I²⁰ of the law to the use of such devices, insofar as Article 32-II provides for a dispensatory regime in the matter of individuals' information.

However, the CNIL recommends that the information measures provided by Article 32-II, namely information about the purpose of the device and the means to object to its insertion, be complied with even though the use of the device would apply only to anonymous data. In any event, the previous section has shown that when a tracking cookie is used, it cannot be anonymous data.

According to the CNIL, clear and comprehensive information should be provided in all cases in order to ensure a full transparency on the use of this type of device. Also, this position is inspired by the spirit of the Directive 2002/58/EC which reminds in its recital 24 that the terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the privacy of the users which must be protected under the European Convention for the Protection of Human Rights and Fundamental Freedoms (see Annex 1 on CNIL notice templates applying to cookies).

From the foregoing, it follows that any actions to access or enter information into the terminal equipment of a user should be possible only if the person concerned is informed in a clear and comprehensive manner about the purpose of this action and the means to object to it.

Besides, **the CNIL reminds that the analysis of purchasing behaviour in order to customize ads targeting Internet users is possible only if the user has been informed in advance, and if the user has been given the possibility to object and even consent if the ad is sent electronically.** The exercise of this right should be made available in a specific way; also it should not prevent the Internet user from making online purchases (i.e. purchasing suggestions proposed by Amazon, based on recent purchases by the user, should be allowed only if the latter has been informed in advance. He should also be able to buy books on the site without information about his purchases being processed for advertising purposes).

Shouldn't the CNIL remind the principle of respect of people's right in case of use of the technology called "tracking cookies"? In this case, it is a real tracking enabling to hound the Internet user's movements on every site displaying ads from the same advertising agency.

It is essential that issues relating to the determination of the data controller, the applicable national law, the data retention time, and the methods for informing people when creating

²⁰ [Added by the translator: Article 32-I: *The data controller or his representative must provide a data subject from whom personal data is obtained with the following information, except where he already has it:*

(1) the identity of the data controller and of his representative, if any;

(2) the purposes of the processing for which the data are intended;

(3) whether replies to the questions are compulsory or optional;

(4) the possible consequences for him of the absence of a reply;

(5) the recipients or categories of recipients of the data;

(6) the rights granted him by Section 2 of this Chapter (rights of individuals in relation to the processing of data);

(7) when applicable, the intended transfer of personal data to State that is not a Member State of the European Community.

If the data is obtained by way of a questionnaire, the information provided for in Sub-sections (1), (2), (3) and (6) shall be directly mentioned on this questionnaire.]

profiles be widely discussed and brought to the attention of economic stakeholders as well as users of the information society services.

In this respect, the conclusions reached by the article 29 working party in its opinion on search engines should be considered.

This opinion clarifies the conditions of application of the European Community rules and makes recommendations in order to improve the protection and the rights of search engines users.

The current practice of these stakeholders is to take into account queries history, user's categorization and geographical criteria. Therefore, depending on the user's behavior and his IP address, a personalized ad can be displayed.

The WP29 also considers that the European data protection rules is applicable to search engines, even if their headquarters are located outside the European Union, under the provisions of Article 4.1(a) et 4.1(c) of Directive 95/46/EC.

The WP29 opinion further explains very clearly the scope of the obligation to inform individuals²¹. It believes that most Internet users are not aware that data related to their queries are processed for targeted advertising purposes. Search engines should, as a consequence, clearly indicate to users what are the data collected about them and what for.

In addition, because of the browser's default setting, *"it is very important that users are fully informed about the use and effect of cookies. This information should be more prominent than simply being part of a search engine's privacy policy, which may not be immediately apparent"*.

Finally, **the WP29 recommends that the enrichment of users' profiles with data not provided by the users themselves should be subject to their consent.** Online targeted advertising generates other questions about data retention time, the collection of sensitive data and the security of processing.

The question of the legal regime applicable to advertising sent through pop-up²² should also be raised. Due to the intrusive nature of this type of advertising, should it be subject to an opt-in (i.e. subject to the prior consent of the Internet user) or an opt-out (the possibility to object to the display of pop-ups)? In this regard, in an answer to a parliamentary question, the European Commission considered that the definition of electronic message covers only messages which are stored in a terminal equipment until they are checked by their recipients, and not messages which "disappear when the recipient is no more online; therefore pop-ups should not be subject to an opt-in"²³.

²¹ Note that the Consumer Code provisions on advertising may apply in this case if there is a lack or bad consumer information. In the United States, the US Bureau of Consumer Protection (the "FTC" Federal Trade Commission) addressed the issue of users' information and recommends that every website collecting data for targeted advertising shall provide to the consumers a clear, concise and friendly notice.

²² The "Pop-ups" or "pop-up ads" are a secondary window which appears before the main browser window without having been requested by the user when surfing on the Internet.

²³ However, in a decision of March 26, 2003, the German Court of Düsseldorf found that pop-ups were messages temporarily stored in the RAM of the Internet user computer and therefore were equivalent to emails. This practice was thus likened to the practice of spam and has been considered as illegal since it had not been previously authorised by the Internet user.

Proposal

The implementation of practices transparent and respectful of individuals' rights must be encouraged among information society stakeholders. It is essential that online targeted advertising be done fairly and that information notices be readable and understandable by Internet users. It seems that many websites still incompletely satisfy the requirement of transparency regarding Internet users' information. **It is the reason why the CNIL could draft template notices and could encourage the adoption of code of good practice by professionals.** The CNIL also proposes to coordinate its action with the *Forum des droits de l'Internet*, for instance, in the development of codes of conduct.

2. Information of the public on the means to control their traces

Part²⁴ of the Internet user's control on targeted advertising requires a real management of tracking cookies. Several stakeholders have understood this and we see the emergence of new tools allowing the Internet user to have more control over cookies.

- Most modern browsers (Internet Explorer 7, Firefox, Safari) have tools allowing to manage cookies, including to block cookies from "third party" sites, i.e. cookies which are displayed by another site than the site displaying the main content (see section II.C). This approach gives correct results.
- Internet Explorer and Firefox browsers enable to create "blacklists" of sites for which cookies should be blocked. It is a very effective but complex tool to implement for non-specialists. Browsers should be improved to make this approach more accessible.
- The latest versions of some browsers have a "private" navigation mode offering a better protection of traces including the automatic deletion of cookies at the end of the browsing session, regardless of their life expectancy.
- Finally, in its solution unveiled in March 2009 of targeting by center of interest, Google has proposed a system allowing users to know and to modify the centers of interest which are automatically assigned to them during their navigation.

These effective technologies are yet rarely used by the public. This is partly due to the complexity of some of them, but also to the lack of awareness of their existence.

The CNIL website has already drawn the attention of Internet users on the trails they may leave, but it also seems appropriate that the CNIL contributes to inform the public on technologies enabling to better manage tracking cookies used in targeted advertising.

Proposal

Measures of awareness and support of the public on issues arising from online advertising should be favoured. **The CNIL could, within this framework, develop on its site educational tools in the form of practical advice to users.**

In 2007, a proposal in the 2007 Belgium Act was also intended to subject pop-ups to the opt-in principle.

²⁴ The cookie is the most used tool to trace Internet users but it is not the only one.

DoubleClick, for instance, sometimes uses other techniques based on simple HTML links. Therefore, the control over cookies will not solve all problems.

C. Promoting products and services respectful of personal data protection.

1. The quality-label advantage

Many websites displaying ads claim to be respectful of data protection. However, only few people take the time to read and understand in detail their data protection policies. Moreover, the Internet user has no indicators to assess their actual veracity.

The quality-label of products or services is a possible answer to this problem. The CNIL has a power to deliver labels since 2004. Nevertheless, as was indicated by the Ministry of Justice in response to a written question asked on 11/12/2008 by the President Türk in the Senate, this new power requires to define regulatory implementation measures and even requires a legislative intervention if the outsourcing of some procedures is anticipated. It is intended to propose an amendment of the law through amendments to the Data Protection Act which will be tabled by M. Warsmann.

In the meantime, the Commission has been involved since 2007 in a European project “European Privacy Seal” (EuroPrise²⁵). This project has helped to define procedures and to evaluate the first products in order to issue a label acknowledging their quality in terms of data protection.

In this respect we can cite the example of the advertising agency “WonderLoop” which was recently subject to an independent expertise and won the European label Europrise^{26,27}. This label emphasizes the compliance of the service with the principles of the European Directive on personal data protection.

Labelling is therefore a tool that the CNIL could use to promote products and services protecting personal data in the context of targeted advertising, at a national level and/or a European level²⁸. Nonetheless, it must be underlined that a “privacy” label²⁹ goes beyond the mere issue of online advertising; it actually encompasses the overall compliance of the law by stakeholders.

Proposal

It is proposed to reaffirm to public authorities the need for the CNIL to quickly implement its labelling power. Beyond the competitive advantage for businesses, a privacy label could help to build Internet users’ confidence in the digital world.

²⁵ The label Europrise has recently awarded the Ixquick search engine that provides Internet search services with strong guarantees on the protection of evidence, particularly by the absence of tracking cookies and by a data retention of IP addresses limited to 48 hours (as opposed to 9 months retention by Google). The advertisement around this label delivery had for consequence to make Ixquick known to a much wider audience.

²⁶ Europrise, the project of European label for personal data protection propose to create a European assessment process enabling to certify the conformity of computing products and services with the European regulation on personal data protection. The label is delivering after an evaluation process that is divided into two specific steps: first an assessment of the product or service by legal and technical experts recognized as such, then a validation of the evaluation report by an accredited certification body. See <https://www.european-privacy-seal.eu/>

²⁷ The CNIL participates to the Europrise project with an “Advisor” status.

²⁸ By becoming for instance a certification authority accredited in Europrise.

²⁹ Note by translator : « label informatique et libertés » in the French original version

2. Promoting standards compliant with personal data protection

Today, all cookies are similar and very little enables to distinguish tracking cookies from other cookies.

Proposal

Efforts could be undertaken in order, for example, to standardize and to distinguish advertising tracking cookies from other cookies

In developing such standards or good practice, together with browser developers, it seems possible to substantially simplify the means of control of cookies available to Internet users. This should be conducted with other authorities of the WP29.

VIII. Conclusion

Targeted advertising and in particular behavioural advertising is at an early stage of development. It is likely to raise a number of challenges with regard to the Data Protection Act.

In particular, the lack of transparency of online advertising systems, as well as the imperfect possibilities for the Internet user to object effectively raise many difficulties.

Although many stakeholders hide behind the fact that the profiling of Internet users would be conducted on an anonymous basis (and would therefore not be subject to the Data Protection Act), it is clear from the analysis done in this report that all systems of targeted advertising on the Internet do process personal data.

In view of the issues raised in this report, the CNIL could:

- **Reaffirm the applicability of European law in this context,**
- **Encourage the adoption of code of practice by professionals and coordinate its action with the *Forum des droits sur l'Internet***
- **Support broadly the principle of active prior consent (opt-in)**
- **Support the development of tools for Internet users to protect their privacy on the Internet**
- **Inform users by developing, for example on the CNIL site, educational tools in the form of practical advice**
- **Conduct audits of advertising on the Internet**
- **Implement procedures for products and services labelling to protect Internet users' personal data, where the regulatory framework allow it**
- **Encourage the implementation of a common reflection, on this theme, with other European data protection Authorities**