Factsheet on **behavioural advertising and privacy**

Online advertising now targeting Internet users' interests

Online advertising has been **growing hugely**, by 15.3% in 2010 alone. It represents 17.7 billion Euros in the European Union.

These adverts are **tailored to Internet users' interests** to ensure that the money invested in advertising is not wasted.

But this type of advertising also has downsides: it is ubiquitous and uncontrolled.

- **Harvesting private information** is a problem: advertising firms use "cookies" or "super cookies" to collect a large amount of data, especially through social networks where the data they gather is on users' identities.

- **Targeting may reach the wrong person**, especially in a family where all members share the same computer. For family organisations with concerns about ethics and privacy this is a big black mark, especially as children are accessing social networks and the Internet at increasingly younger ages.

However, browsers can help to block advertising and **protect against tracking**. The three main browsers –and their pros and cons– are reviewed below.

How browsers can help protect privacy

**Firefox**

Firefox was the first browser to offer a "**Do Not Track** (DNT) feature". It is a straightforward system: the browser sends a signal to any website you go to asking it to disable any tracking requests from third-party websites. In fact, it is recommended by the United States Federal Trade Commission.

- Its main pluses are: it is easy to use, and there may be legal consequences for websites who ignore the request. Users can also install add-ons and extensions.

- On the minus side, it cannot provide full protection: most websites are still ignoring the signal in practice.

**Chrome**

Google's strategy is focused on a plug-in entitled "**Keep My Opt-Outs**" which acts as a black-list blocking a preset number of websites.

- The plug-in provides quick protection against tracking which is more effective than Firefox's although the block-list is not as comprehensive as those of Firefox and Internet Explorer. It has the added advantage of being a highly customizable browser: so users can opt for alternative plug-ins to the Google one.


However, while this plug-in comprehensively blocks all Microsoft advertising and tracking addresses, it only blocks one single Google advertising and tracking website. It has been also criticized for not supporting the "Do not track" feature.

Internet Explorer

Like Firefox, this includes a "Do Not Track" feature which is on by default (the proposal for a Data Protection Directive mentions "privacy by default settings"). It also has additional features like tracking protection lists that are built into the browser. Black-lists, however, are not customized.

- This is a good thing because it gets users actively involved in setting up their tracking protection features.

- On the downside, it requires a degree of awareness and expertise from consumers. For this reason, Microsoft plans to provide useful information on how the lists work. Also, some lists - like the TRUST list - have been criticized, while others – like the Easy-list - seem quite complete. Finally, installing more than one list can be counterproductive (the "allow" rule will prevail if two lists conflict).

A word of caution

Even with these protection features, some limitations have to be kept in mind:

- Changing websites to recognise the "Do Not Track" feature will take time.

- New websites spring up every day, so black-lists have to be constantly updated.

Consumers need to make sure they have chosen the right list because some lists allow all advertising.

- Tracking protection requests do not work if you go straight to the domain where the filtering is done (e.g., going straight to the Google homepage).

- Setting up tracking protection can restrict certain things you can do online, like sharing newspaper articles or videos on social networks.

Conclusion

Each browser uses different strategies working towards the same end. Consumers are better informed about tracking and the collection of private data, and so prompted to find out more about the different lists, for example.

COFACE therefore urges parents to turn on these features in order to safeguard young children against advertising and tracking.

But even more important than technical tools is good parenting: children need to be made aware about protecting their privacy to keep staying safe online in mind.

The Confederation of Family Organisations in the European Union (COFACE) is a pluralistic organisation, which aims to promote the family dimension of European policies, programmes and initiatives.

Contact: Tel: +32 2 511 41 79 | E-mail: secretariat@coface-eu.org | Website: www.coface-eu.org

COFACE is supported by the European Union Programme for Employment and Social Solidarity - PROGRESS (2007-2013): http://ec.europa.eu/progress