DATA COLLECTION, TARGETING AND PROFILING OF CONSUMERS ONLINE

BEUC discussion paper

Contact: Emilie Barrau – digital@beuc.eu

Ref.: X/010/2010 – 15/02/2010

BEUC, the European Consumers' Organisation
rue d'Arlon 80, 1040 Bruxelles - +32 2 743 15 91 – www.beuc.eu

Summary

This paper is a first attempt to address concerns raised by online marketing to consumers – including new techniques such as behavioural targeting and profiling. Today, consumers have almost no control over this complex "media and marketing ecosystem". BEUC is not inherently opposed to the tracking and profiling of consumers online and the targeting of marketing, if it is done in a controlled and transparent manner. We thus believe it is high time to assess what impact these new marketing techniques have on society at large, and in particular on transparency and digital diversity of offers, competition and how consumers are treated online.

BEUC calls on the European Commission to consider the following points:

- Consumer should retain control over their data. Consumers' control should be real, cost-effective, easy to exercise and persistent whenever possible. It is critical to obtain consumer's meaningful consent.
- To achieve consumers' control and choice, transparency is a prerequisite. The fairness, readability and transparency of privacy notices need to be of a high standard; though privacy notices alone will not improve consumers' awareness.
- Alternative business models using privacy and security by design should be encouraged.
- Online targeting and profiling should fully respect data protection rules when these techniques collect and use data on tastes and behaviours that may be linked to an identified or identifiable person.
- Existing laws – when enforced - are probably appropriate to tackle most consumer concerns raised by profiling and targeting. The Commission should carry out a legal gap analysis to identify how the current European set of rules could apply and where, if necessary, new measures may be needed.
- BEUC considers that a "one size fits all" solution is neither adequate nor efficient to tackle all profiling and targeting marketing techniques. One should look at whether these techniques could lead to potential consumer detriment and meet the 'reasonable expectations' of an average or typical consumer.
- Vulnerable consumers that are more sensitive to suggestion and are an easy target for advertisers, and in particular children and young people, should not be targeted by websites using profiling and behavioural marketing techniques. Moreover, collection of sensitive data always requires an opt-in.
- All online businesses should have an obligation to indicate to all consumers alike a catalogue price or a reference or range price.
- Any detrimental offer based on online profiling and targeting should be banned. Traders may offer subsequent differential better offers to consumers if the basis on which the offer has been made is transparent and if the individualised price is clearly indicated along the catalogue price or reference price.
- Stealth advertising and advertorials that are not clearly displayed as advertising should be banned.
- We ask for deep packet inspection (DPI) methods and e-mail scanning technologies that aim at serving targeted ads to be banned.
- Strong liability and public accountability rules are needed. In particular relation of a business with third parties should be clearly revealed.
- Respect of consumers' rights and safeguard of consumers' data is a contractual obligation on the part of business. Business should be sanctioned for lack of diligence and for the non-respect of contractual obligations. Consumers should be compensated for financial detriment they suffer as a result of data breaches or unauthorised use of their data.

"Tools must now be developed that balance the interests of business with that of the consumers. This means two things: the respect of users' right to control their public exposure; and the obligation to protect them against abusive and risky practices targeted at them" - Commissioner Kuneva, Roundtable on Online Data Collection, Targeting and Profiling, 31 March 2009

PRELIMINARY REMARKS

- **A complex ecosystem – look at the bigger picture**

Targeting and profiling have to be addressed as part of the media and marketing ecosystem. Both are inextricably linked to the range of marketing applications on various platforms that are designed to provide targeted offers/information, to influence consumer decision-making and also foster further data collection. Techniques such as the use of neuromarketing[1], immersive rich media i.e. video that allow user interaction, viral targeting via social networks, retargeting and location-based targeting for mobile phones are all part of this "media and marketing ecosystem". Behavioural targeting, which covers a series of technologies that collect and organise data to reveal consumers' presumed online behaviours and interests and serve them targeted ads, cannot be seen in isolation[2]. Today, consumers have limited control over this complex ecosystem as all these techniques are not transparent or sometimes are even invisible.

- **Several layers of data collection**

When surfing the Internet, consumers' data are collected at different levels: by Internet Service Providers (ISPs)[3], web browsers, email scanning, publishers, affiliation companies, social network platforms, ad-serving agencies and data aggregator companies. All these layers are increasingly intertwined due to a growing vertical integration which leads to increased data collection. In addition, there is a will to expand data collection to new platforms i.e. to connect online, offline and in-store consumers' buying behaviour[4]. The impact of all these layers and sources of information on consumers' data protection and privacy – and in particular the confidentiality of communications - needs to be fully considered and assessed.

- **Personal data has an inherent economic value**

As rightly underlined by Commissioner Kuneva: **"***personal data is the new oil of the Internet and the new currency of the digital world*"[5]. The Internet is not "for free". Consumer data is becoming a valuable good[6]. For instance, figures from online publishers show that advertising space sold to behavioural marketing ad serving companies is worth six to ten times more than if the space was sold to traditional online advertisers[7].It is even a business on its own; online data brokers and other companies openly advertise that they sell consumers' data. Consumers' data quite clearly has a significant value that must be treated carefully.

---

1 "Gain consumers' attention; engage their emotions; stimulate retention in their memory; build awareness, provoke persuasion and achieve novelty", NeuroFocus, Advertising Effectiveness Product Sheet, 2008.

2 In addition, online advertisers will use more and more behavioural targeting. In 2008, 24% of online advertisers are using it. By 2020, 85% of online advertisers will be using behavioural targeting (source: AudienceScience - http://www.audiencescience.com).

3 See the Office of the Privacy Commissioner of Canada website – collections of essays on Deep Packet Inspection at http://dpi.priv.gc.ca/

4 Catherine Dwyer, Behavioural Targeting: A Case Study of Consumer Tracking on Levis.com, August 2009.

5 Commissioner Kuneva, Roundtable on Online Data Collection, Targeting and Profiling, 31 March 2009.

6 It was estimated that in 2009 Facebook would earn 5$ per user in advertising revenues, which multiplied by the millions of users, gives an impressive sum (IPA/FF estimate). Similarly, 1,000 impressions bought using BlueKai data can cost $4 to $15 (http://www.xplusone.com/media/042009.html). BlueKai is a data aggregator and exchange company.

7 From Reed Elsevier, publishing group.

PROFILING AND TARGETING EFFECTS

Targeting and profiling techniques are not as such harmful for consumers; they can even bring forward consumer benefits, if adequately designed. However, we consider that many existing practices lack the necessary transparency and accountability.

The vast majority of consumers at the moment do not realise information about their web activities is being collected. Some may like getting targeted information that matches their (presumed) interests - many however do not realise that they might not be getting the full range of options available because of e.g. the salary data or home-ownership data, and more crucially, records of previously visited internet sites, already in the hands of some companies. Consumers do not control where their data is going and would not know who to address in order to exercise their rights under the relevant Data Protection laws. From another angle, privacy issues may also arise when several users share the same computer and that one receives advertisements to sites which another user has been on but which he/she would rather keep private.

Also, the generalisation of the creation of artificial social categories may affect how consumers are treated online. Profiling and targeting create a risk of being pigeonholed into a narrow spectrum of advertisements which do not reflect the consumer's full range of interests. Targeting and profiling also have an impact on transparency, and ultimately could have a negative impact on digital diversity, as the tendency to generalise the results from profiling might lead to a diminution of preferences, differences and values[8].

From a competition angle, there is a risk that companies which monopolise data collection and have significant control over a vast amount of the total advertising inventory on the Internet could abuse their position, for instance by charging higher costs to advertisers and lower advertising revenues for web publishers. This would be at the expense of other companies and would ultimately impact on consumers' choice.

CONSUMERS' EXPECTATIONS

European consumers are concerned about data protection, privacy and security issues. The latest Eurobarometer survey[9] revealed that 82% of respondents who were Internet users thought that data transmission over the Internet was not sufficiently secure. Most European Internet users were also not familiar with tools or technologies that helped to limit the collection of personal information while using the Internet.

Sharing data for commercial use can often be seen as a constraint rather than as a real consumer choice.

Today, consumers give away their data for use of a service online and the advertising company reaps the economic benefit. Internet users are thus paying for services with their data. However, if the exchange of consumers' data is the only accepted currency for a particular service, there is no real choice for consumers. Also many service providers only allow consumers to access to their services if they agree that their data can be used for marketing purposes. All these practices potentially lead to a loss of consumers' control over their own data. We are not inherently opposed to consumers entering such an

---

8 Mireille Hildebrandt, Serge Gutwirth, Profiling the European citizen - cross-disciplinary perspectives, 2008, Springer.

9 Eurobarometer survey on data protection in Europe (February 2008).

exchange for a 'free' service, or other tangible benefit, but it must be ensured that it is absolutely transparent from the outset that this exchange is taking place, that the data is being collected, what it will be used for and how long it will be retained. Wherever possible, an alternative form of currency should be offered if there are no alternative services in the market place. There are already business models in certain online markets which have provided consumers with similar choices, for example, Spotify[10] offers its services for free if consumers sign up to advertising, or they can pay for the service and have no advertising.

Specific studies should be carried out **to quantify, evaluate and assess the extent of practices that oblige consumers to give their consent to their data being used**. We predict that there are significant benefits for business but at a cost for consumers that have not yet been quantified. Sustainable business models on the Internet that could run without requesting consumer data – for example based on anonymous credentials[11] - need to be researched and developed.

- **Children and young people**

Contrary to what is often claimed, young people are not different; they also care about the protection of their privacy. A recent scientific report demonstrates that 82% of young people are very concerned that personal information is used without their knowledge, 75% that their identity is reconstructed using personal data from various sources and 69% that their views and behaviours may be misrepresented based on their online personal information[12]. While they acknowledge the risks, young people do not take steps to protect themselves. They hardly ever give misleading or wrong information; they do not always give a minimum of information or adopt other identity-shielding strategies[13]. The digital world has the ability to reach consumers emotionally; in particular when it comes to children and young people that are more sensitive to peer-pressure and thus become easy targets for advertisers.

Specific rules should be put in place for the protection of children and young people – in particular due to their lack of critical judgment and understanding of marketing. In fact, recent neuroscience research conducted both in the EU and the US[14] suggests that, contrary to previous beliefs, children over 12 do not have adult-like understanding and critical judgment of marketing.

Online marketing practices that have a negative impact on children and young people's cognitive and emotional development should be prohibited – this is particularly relevant in the context of the childhood obesity epidemic.

CONSUMER POLICY ISSUES

We believe that the current laws – data protection laws as well as more "typical" consumer protection laws – are appropriate to tackle most of the consumer concerns raised by profiling and targeting. In particular, the application and enforcement of the Unfair Commercial Practices (UCP) Directive to such marketing practices could help ensure consumers' rights are fully respected. The Directive on Unfair Contractual Terms could

---

10 See http://www.spotify.com/en/

11 See the work of the Privacy and Identity Management for Europe (PRIME) and PRIMElife projects financed by European Commission; www.prime-project.eu and www.primelife.eu

12 Scientific report 'Young People and Emerging Digital Services', 2009: http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=2119

13 Scientific report 'Young People and Emerging Digital Services', 2009: http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=2119

14 See TACD resolution on online marketing to children, www.tacd.org

also be relevant. We therefore **call on the Commission to carry out a legal gap analysis** to identify how the current European set of rules could apply (e.g. to third party cookies) and where, if necessary, new measures need to be taken. In addition, the Commission should **develop guidelines** on how the UCP Directive, the Unfair Contractual Terms Directive but also the Data Protection Directive (95/46/EC) apply to online data collection and marketing practices.

- **Profiling, targeting and the UCP Directive**

Behavioural advertising has a bigger impact on consumers than traditional advertising. A recent study shows that the combination of contextual and behavioural targeting increases purchase intent, brand favourability and awareness among consumers by up to 70%[15]. Behavioural advertising may have the potential to impact on the buying decision of a consumer. In particular, practices that are surreptitious and unusual could potentially have a much bigger impact on consumers. For instance, some companies already target offers based on psychological profiling[16]. Similarly, the use of neurosciences for online marketing purposes should be monitored from an ethical viewpoint. Finally, behavioural advertising may have the potential to increase information asymmetries between the consumer and the professional; the consumer is in a weak position as the business knows far more about him/her that he/she knows about the business.

- Behavioural advertising: a form of undue influence?

Through profiling and the information gathered by Internet companies, consumers could be at a disadvantage when a business has valuable information on their buying habits and behaviours.

Privacy protects the autonomy of the consumer, and preserves his/her independence and free choice in decision processes[17]. Therefore, under certain circumstances, tracking of consumers – might be seen as undermining their autonomy.

In some circumstances, **behavioural advertising may qualify as "undue influence"[18] under the UCP Directive**. First, there is a position of power: the advertisers know a lot about the consumers - even information that the consumers do not intend to disclose - while consumers hardly know what is going on. Then, the repetitive aspect – especially through retargeting – may put pressure on the consumers. Furthermore, the selection of advertisements – based on the presumed consumer interest - may prevent the display of other advertisements and reduce consumer choice. Consumers might thus be pushed to take an economically unsound decision (e.g. as they might not be able to compare prices of other advertisements). The qualification of behavioural advertising as "undue influence" will nevertheless very much depend on the specificities of a particular case.

- Stealth advertising and advertorial

Commercial information must be clearly identifiable as such in order to avoid misleading consumers.

---

15 Jumpstart Automotive Media Inc. and AudienceScience case study, 2009, http://www.marketwire.com/press-release/Jumpstart-Automotive-Media-980713.html

16 The website hotels.com – for instance – used the results of www.Youniverse.com – a website were consumers can "discover their VisualDNA" to target offers based on the psychological profile of visitors.

17 Catherine Dwyer, Behavioural Targeting: A Case Study of Consumer Tracking on Levis.com, August 2009

18 "Undue influence" in the UCP Directive "*means exploiting a position of power in relation to the consumer so as to apply pressure, even without using or threatening to use physical force, in a way which significantly limits the consumer's ability to make an informed decision*".

Stealth advertising – i.e. clandestine marketing – is a misleading commercial practice and therefore **should be banned**.

Advertorials – i.e. mix of editorial and commercial content - **should be clearly displayed** as advertising to consumers; **if not, it should be considered as misleading commercial practices *per se* under the UCP directive**[19]. For instance, running fake blogs about a business or writing (or to pay someone to write) commercially-motivated reviews of a company without making clear the commercial intent, should be considered misleading advertising and thus must be banned under the UCP Directive[20]. Similarly, own brand websites (particularly popular with children) and other type of online marketing techniques such as advergames, viral advertising and others should be considered in the light of the UCP Directive.

In addition, under European legislation, Directive 2000/31/EC on e-Commerce and Directive 2007/65/EC on television broadcasting activities also prohibited surreptitious or misleading commercial communications. We therefore invite the Commission to analyse whether the relevant articles of the above-mentioned directives could also apply to some online marketing practices.

- No targeting of vulnerable consumers

Vulnerable consumers, i.e. children, people vulnerable due to their mental or physical infirmity, age or credulity, **should not be targeted** by websites using online profiling and behavioural marketing techniques. To some extent, the provisions of the UCP Directive may be helpful in this respect[21]. Specific additional rules should be put in place for the protection of children and other vulnerable consumers. In particular, the practice of making children agree to the use of their data for marketing purposes before they can access and use a service should be forbidden[22]. Children and young people cannot give informed consent as they cannot be required to read and understand the highly complex terms of condition/privacy notices.

In addition, we would like to stress that there should be **no targeting of adverts on** tobacco, drugs, alcohol, pornography, medical conditions, gambling or **any sensitive areas** for instance targeted at those suffering from illness, based on financial status or personal beliefs.

- **Price individualisation**[23]

Profiling technologies allow unparalleled kinds of social sorting and segmentation which could have undesirable effects.

Today, companies are able, via the enhanced possibilities of profiling consumers, to discriminate against consumers i.e. by offering the same products at different prices based on individual users' online profile. Such practices already happen on the Internet. A retail photography website, for example, charged different prices for the same digital cameras and related equipment, depending on whether shoppers had previously visited popular price-comparison sites[24]. The same practice was used by a very well-know online

---

19 Annex 1, point 22 of the UCP directive states that "*falsely claiming or creating the impression that the trader is not acting for purposes relating to his trade, business, craft or profession, or falsely representing oneself as a consumer*".

20 See in particular point 11 in annex I of the UCP Directive.

21 See annex 28 of the UCP Directive that prohibits "a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them".

22 See TACD resolution on online marketing to children, www.tacd.org

23 We understand price individualisation as offering the same product at a different price based on online profiling.

24 "Open to Exploitation", Annenberg Center, University of Pennsylvania, 2005.

retailer that offered a MP3 player with a $50 discount for customers who had compared prices on a "bargain-hunter" website[25].

As provided under Directive 98/6/EC on Price Indication, the selling price and the unit price shall be indicated for all products offered by traders to consumers in order to improve consumer information and to facilitate comparison of prices. These principles should not be precluded in online sales.
Therefore, **all online businesses should have an obligation to indicate to all consumers alike a catalogue price or a reference or range price**.

This would not preclude traders to offer **subsequent differential better offers** to consumers **under the cumulative conditions that:**

- **the basis on which the offer has been made is transparent** (i.e. on hidden (partial) profiling and tracking);
- **the individualised price is clearly indicated along the catalogue price or reference price**.

On the contrary, we believe that **any detrimental offer based on online profiling and targeting should be banned**. In fact, price individualisation may lead to higher prices as business could potentially try to get away with maximum prices. For instance, prices offered to an impulsive buyer could be higher than those offered to buyers whose profile shows that they usually visit different sites before purchasing.

CONSUMER CONTROL, CHOICE AND FAIRNESS

As stated by Commissioner Reding, "*European privacy rules are crystal clear: a person's information can only be used with their prior consent. We cannot give up this basic principle, and have all our exchanges monitored, surveyed and stored in exchange for a promise of 'more relevant' advertising!*"[26]. Under EU law, **it is a consumer right not to be targeted** and not to have personal data collected for commercial purposes. Currently, consumers have limited opportunity to choose or to control the dissemination of their data online. They do not know why they see a specific ad when surfing the Web and they are not told which information a company has about them. **Consumers should remain in control of their data**.

It is no longer necessary to know someone's actual name or street address to identify – via cookies, IP addresses and other online targeting techniques – how a particular person interacts online[27]. Any data can become personal. As a result, we believe that **online targeting and profiling should fully respect data protection rules, when these techniques collect and use data on tastes and behaviours that can be linked to an identified or identifiable person**[28]. This includes, amongst other things, the respect of data protection principles such as having the minimum amount of data kept for a minimum time period.

Moreover, one should think that consumers' growing feeling of loss of control over their data may ultimately lead to the rejection of behavioural advertising altogether – which would have a big impact on the advertising industry's revenues and investments.

---

25 Web sites change prices based on customers' habits, CNN, 24 June 2005: http://www.cnn.com/2005/LAW/06/24/ramasastry.website.prices/

26 Citizens' privacy must become priority in digital age, says EU Commissioner Reding, IP/09/571, 14 April 2009.

27 See in particular the Article 29 Working Party opinion 1/2008 on data protection issues related to search engines.

28 Please see CNIL (French DPA) opinion on online targeted advertising, February 2009.

- **Consumer control**

To achieve consumers' control, **transparency is a prerequisite**. However, today's online marketing and commercial practices lack the necessary transparency.

- Privacy notices

"*The burden placed upon individual to read these policies stretches the limits of acceptability*"[29]. The vast majority of consumers do not currently read privacy notices due to their length, complexity and complicated language[30]. The notices fulfil legal business obligations rather than informing consumers. They are not always easy to spot on a website nor in a language the consumer can understand.

In addition, privacy notices do not always reflect what is really going on. Often, privacy policies are partial and only include information on the collection of what a specific business considers personal identifying information (PII); all other data collected (e.g. location, IP addresses, articles read, search keywords…) is not mentioned[31].

Another important issue is the relation of a business with **third parties**. Such **relations should be clearly revealed** – including what third parties intend to do with the data they collect, receive, exchange or buy. In this context, the Commission might consider the opportunity to set up **joint and several liability rules** between a business and third parties in case of breach, in order for the consumer to be able to claim full compensation for the damage suffered from any of them[32]. In particular, as offline, publishers should be held accountable for online advertisements. Currently, many privacy policies of online websites using behavioural marketing for their advertisements disclaim any liability.

Existing privacy policies discourage people from reading all the obligations forced upon them and exercising their rights[33]. **Fairness of terms needs to be improved and policy notices need to be easily accessible and clearly displayed in plain and intelligible language**. Notice must be provided before or at the point of collection (including secondary purposes, whether data is shared with or sold to third parties, who these third parties are and what they intend to do with the data…).

Several options could be explored to improve transparency: prominent ad-tracking disclosure; use privacy seals such as the EuroPrise initiative[34]; development of notification standards; layered privacy notices i.e. first providing the user with a summary of key privacy points, and then providing access to the full privacy policy for those who wish to access more detailed information; mandatory external privacy audits, use of Transparency

---

29 The London School of Economics and Political Science (LSE), from legitimacy to informed consent: mapping best practices and identifying risks, a Report from the Working Group on Consumer Consent, May 2009.

30 A study produced by the Consumer Council of Norway documents that consumers generally do not understand the terms of service that is offered by their favourite social networks: http://www.sintef.no/upload/Konsern/Media/Person%20og%20forbrukervern.pdf

31 Catherine Dwyer, Behavioural Targeting: A Case Study of Consumer Tracking on Levis.com, August 2009. See for instance the example of the Levis' website.

32 For instance, in Denmark a sector agreement has established a joint-liability between the mobile phone companies or Internet Service Providers and third parties such as mobile content providers. The mobile company takes the responsibility for the services provided by third parties and in return gets a percentage of the revenues generated by the services (e.g. on ring tones, virtual websites sale, Facebook applications etc...).

33 The above-mentioned Norwegian study reveals that 73% of users aged 15-30 rarely or never read the terms of service (TOS). Only 4% of these users claim to read terms of services routinely. During the study, a selection of TOS were put under evaluation and measured against some key consumer expectations, for a general overview of the results, see: http://forbrukerportalen.no/filearchive/matrix_terms.jpg

34 The European Privacy Seal certify IT products and IT-based services privacy compliance with European data protection regulations - https://www.european-privacy-seal.eu/

Enhancing Technologies (TETs)…. Business could also conduct focus groups and surveys to find out what the most efficient way to informed consumers is.

However, increased **transparency of privacy notices alone will not improve consumers' awareness** and resolve the current issues. In addition, it must be clear that posting policy notices on a website is not sufficient to conclude to have received informed consent from a consumer. The burden to demonstrate that consumers are well-informed should be on the business.

Consumers' trust cannot be enhanced if they are not given control. Young people, for example, ask for tools that give them more direct control of their own privacy identity data[35]. The question that needs to be answered however is how this control should be exercised.

- **Consumer meaningful consent**

Not all online data collection practices (e.g. simple session cookies) are linked or aim at collecting consumers' data for commercial or marketing purposes.

While it is important to note that there are several ways to validate the processing of personal data, consumer's consent is very often used.

BEUC believes that the means of implementation of consent for online targeting and profiling of consumers should be flexible and user-friendly – in particular as independent studies on the acceptance of European citizens of such practices and their effects are still missing. What is critical is to obtain **consumer's meaningful consent** i.e. "free, informed and specific". We are conscious of the fact that "a one size fits all" approach is neither adequate nor efficient.

We therefore call on the European Commission to **commission studies both on consumers' response to targeting and profiling marketing techniques and on the effects of such practices on consumers' behaviour** as soon as possible.
For instance, we believe that practices could be assessed against the two following criteria:

1. An analysis of the **potential consumer detriment** linked to a specific practice/technique. For instance, consumer detriment could be interpreted as limiting consumers' choice or access to services based on individual users' online profile…. Similarly, an online marketing practice would cause a consumer detriment when it qualifies as "undue influence"[36] under the UCP Directive.

2. An evaluation of whether a practice/technique meets the **'reasonable expectations'** of uses of his/her information by an average or typical consumer or by the average member of the group when it is directed to a particular group of consumers[37].

The type and amount of data collected and stored and the objective(s) underlying the collection of the data will be critical in determining whether a practice meets the expectations of an average consumer. For instance, we believe that an average consumer

---

35 Scientific report 'Young People and Emerging Digital Services', 2009: http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=2119

36 "Undue influence" in the UCP Directive "*means exploiting a position of power in relation to the consumer so as to apply pressure, even without using or threatening to use physical force, in a way which significantly limits the consumer's ability to make an informed decision*".

37 An average consumer is to be understood as a reasonably well-informed and reasonably observant and circumspect consumer, taking into account social, cultural and linguistic factors. (Recital 18 of the UCP Directive).

does not expect his/her data to be collected and shared or even sold by a website he/she visits to third parties across the web. Similarly, a consumer does not expect ad serving networks to combine any of the tracking data they collect about users with any data provided by retailers – such as purchase history, postal address etc.

In any case, it is clear for us that in the following cases, a high level of consumer protection is necessary:

- We ask for a strong **opt-in** for any collection of sensitive data; consumer's **sensitive information** should only be collected after the consumer has given his/her express prior consent. Moreover, sensitive information should never be used to target or profile consumers.
- As expressed above, **vulnerable consumers** i.e. children, people vulnerable due to their mental or physical infirmity, age or credulity **should not be targeted** by online behavioural marketing techniques.
- Due to the large amount of data collected across the web, the strong potential consumer detriment and above all the violation of the fundamental right to the confidentiality of communications, we ask for **deep packet inspection (DPI) methods[38] and e-mail scanning technologies** that aim at serving targeted ads to be **banned**[39]. If the post office is not allowed to open and analyse your letters in the offline world, why should your ISP or your email account provider be authorised to do so?

In addition, the Commission should as soon as possible start reflecting on the best way to implement the relevant provisions of the revised e-Privacy Directive 2002/58/EC in a practical and user-friendly way.

Consumer control should be real, cost-effective, easy to exercise and persistent whenever possible. We know that consumers use the option by default; very often they will not take complicated and time-consuming steps to protect their privacy.

- Opt-out cookies and browser settings

Some companies have introduced **opt-out cookies** for behavioural targeting[40]. This is far from being a panacea as consumers do not know that this is possible. Even if a consumer knows about opt-out cookies, he/she would have to search and find the various opt-out cookies that are available on the numerous ad-serving companies' websites he/she visits. Then, such cookies – when they are not persistent[41] - are deleted when consumers erase cookies and thus need to be reinstalled. Moreover, a website may be able to restore deleted tracking cookies through the use of cookie alternatives such as "flash cookies" that are used on most popular websites – not to mention that the use of deep packet inspection methods would not be covered.

Another potential solution would be to use **browser settings** to set a high level of privacy. However, it should be noted that it can be easily circumvented as it is very likely

---

38 Deep Packet Inspection refers to the use of network equipment to intercept and modify, examine, restrict, or copy the content of data communications. (definition from www.nodpi.org)

39 Please note that Which? believes that Deep Packet Inspection should be an explicit opt-in, with clear notice provided prior to data collection. They would also like to see a member benefit offered to the consumer in exchange for their tracking data, leaving the choice up to the consumer. Opt-outs should be available at any time, data collected should only be retained for a short period and data collected should be limited to only that which is necessary (therefore no personal identifiers should be held by the company operating the DPI).

40 Please note that with opt-out cookies, consumers would only opt-out on receiving targeted advertising, not on having their data collected.

41 To our knowledge, Google is the only company that has implemented a persistent opt-out cookie. This option is very recent.

that technology will develop to find alternative means around such barriers. For instance, if a browser is set not to accept third party cookies, ad serving companies are developing first party cookies to circumnavigate this rule. In particular, **'flash cookies'** are problematic as they are stored in a different location than regular http cookies and are not removed if you delete cookies from within your browser. Even the 'Private Browsing' mode recently added to most browsers still allows 'flash cookies' to operate fully and to track consumers[42].

The burden to protect oneself should not be put entirely on the consumer. For instance, a consumer should not see his/her responsibility engaged for taking or not taking precautions through their browser settings. Consumer-friendly alternative business models for online marketing need to be encouraged and consumer friendly technical solutions should be put in place to help consumer choice and facilitate consumer control.

- Privacy and security by design

Privacy and security by design and the use of Privacy Enhancing Technologies (PETs) is a way to enhance consumer control and facilitate consumer choice.

Privacy and security by design needs to be integrated in new online marketing business models. For instance, Ixquick, a search engine that does not collect IP addresses, can be seen as a step in the right direction[43]. Similarly, there is a trend towards facilitating user control through browsers e.g. Internet Explorer 8 *InPrivate* filtering, Firefox Private Browsing, Google Chrome's Incognito…[44]. Privacy-by-default settings in browsers - as the majority of users rely on default settings – like the automatic deletion of cookies and temporary Internet files at the end of each browsing session, but also browser ad-ons like TACO (Targeted Advertising Cookie Opt-Out)[45] or Better Privacy[46] should be further researched, developed and widely publicised.

When it comes to cookies, we believe that they should be designed to expire after a certain limited period, and the data collected via the tracking cookies – which should be limited to that which is strictly necessary to fulfil the purpose of online behavioural marketing - should also be deleted after a certain limited time. IP addresses should not be retained and all steps should be taken to irreversibly anonymise as soon as possible any data collected i.e. with no possibility to de-anonymise data at a later stage[47].

---

42 UC Berkeley research study on flash cookies http://www.law.berkeley.edu/institutes/bclt/about/about_news_08-17-09_3.htm

43 Ixquick search engine does not collect IP addresses - http://www.ixquick.com/

44 LSE Advanced Internet Policy Report on Online Advertising: confronting the Challenges, May 2009. As mentioned above, browsers 'Private Browsing' mode still allows 'flash cookies'.

45 TACO is a Firefox add-on that sets a number of permanent, generic, non personally identifiable opt-out cookies in the browser, which will prevent 90 different online advertising networks from subjecting users to behavioural advertising - http://taco.dubfire.net/

46 Better Privacy is a Firefox add-on that allows you to view, delete and block the use of "Flash cookies," which are a method of tracking used by some ad-delivery companies - https://addons.mozilla.org/en-US/firefox/addon/6623

47 In the summer of 2006, a service provider published a sample of queries and results of some 650.000 users during a 3 months period. Even though AOL had replaced the names of the users by a number, journalists found out these results could often be traced to individual users, not only because of so-called 'vanity searches' (people searching for information about themselves) but also by combining several queries by a single user.

- Privacy Enhancing Technologies (PETs)

PETs could help enforce the principle of data minimisation by limiting the collection of personal data and serve as identity management instruments. When developed, PETs should apply the PRIME principles such as e.g. design must start from maximum privacy [48]. To be used by consumers, PETs would need to be **affordable, user-friendly, interoperable and accessible to all**. PETs would even be more effective if they were employed not only on consumers' computers but also at companies' or Internet Service Providers' servers level.

As rightly summarised by the Working Group on Consumer Consent [49]:
"*In the realm of online advertising there must be some means of informing users that their personal information is being processed for advertising purposes, informing the nature of that processing and the risks therein, and offering the means to give consent, without overburdening the consumer or introducing new risks*".

REDRESS OF CONSUMERS' DETRIMENT

A company is dependent on its customers and its reputation/brand image. Trust is a company asset. More and more companies damage their reputation due to privacy scandals or the massive loss of consumer data[50]. Once illegal activities or numerous data loss are discovered, it will be harder for a company to hide a bad reputation and to regain consumers' confidence. **Privacy is part of the Business-to-Consumer (B2C) equation.** It should be seen as a competitive advantage. For instance, Amazon UK was the first to announce that it will block the online advertising system Phorm to scan its web pages to produce targeted ads[51].

Notwithstanding the economic value of trust, **the respect of consumers' rights and safeguard of consumers' data is a contractual obligation on the part of business**. Companies and organisations that collect consumer data should be held accountable for abuse of data that they have been entrusted with in case of security breaches, loss, alteration, unauthorised disclosure or access to the data. Such breaches should be published. In addition, the sale of consumers' data without the knowledge and consent of consumers should be prohibited. Business should also be held responsible in case a consumer suffers an economic detriment based on wrong information/bad profiling.

Business need to be sanctioned for lack of diligence and for the non-respect of contractual obligations. Last year the German Federation of Consumer Organisations (vzbv) was able to buy six million sets of consumer data on the black market for 850 Euros. The seller of this data was only punished with a fine of 900 Euros. Sanctions need to have a deterrent effect. **Strong liability and public accountability rules are needed**.

Business should also **compensate consumers for any detriment they may suffer as a result of data breaches or unauthorised use of data.**

---

48 This includes design must start from maximum privacy; explicit privacy governs system usage; privacy rules must be enforced, not just stated; privacy enforcement must be trustworthy; users need easy and intuitive abstractions of privacy; privacy needs an integrated approach; and, privacy must be integrated with applications- https://www.prime-project.eu/about/principles/

49 LSE, from legitimacy to informed consent: mapping best practices and identifying risks, a Report from the Working Group on Consumer Consent, May 2009.

50 For instance, T-Mobile, the largest mobile operator in Germany, had to admit that 17 million customer data sets were copied and stolen in 2006.

51 BBC News website, 15 April 2009, http://news.bbc.co.uk/1/hi/technology/7999635.stm

A collective judicial redress instrument (“group action”) in Europe will ensure that consumers can exercise their right to be compensated for the damage they have suffered. Given the relatively low amount of money involved and the fact that moral damages are difficult to quantify, consumers will not go individually to court. If such a measure existed, it would also provide an incentive for companies to abide by the law. It would truly close the consumer protection web.

END