DE GRUYTER OPEN

Wroclaw Review of Law, Administration & Economics

ONLINE BEHAVIOURAL ADVERTISING AND THE PROTECTION OF CHILDREN'S PERSONAL DATA ON THE INTERNET

*AGATA JAROSZEK**

INTRODUCTION

The paper discusses problems emanating from the current and planned legal framework of the European data protection of children that have emerged and have to be addressed, particularly with regard to the social impact that information and communication technologies have on the way children communicate and make choices online. Given that such problems are not only confined to European countries, approaches to regulating children's privacy on the internet from outside the EU are also discussed where relevant.

While in Europe privacy is protected as one as the fundamental human rights that deserves legal safeguards enshrined in the volume of laws that establish comprehensive sets of right and responsibilities for states and individuals, in the United States personal data are perceived primarily as a commercial commodity[1], thus resulting in the adaptation of a diverse and targeted approach based on the Fair Information Practices Act (FIPA model of data privacy protection)[2]. However, it is inevitable that both approaches need to establish long-term policies for the protection of minors (children) and more vulnerable members of societies on the Internet, in particular in the area of online behavioural advertising and other marketing techniques that aim at profiling of individuals.

I. ONLINE BEHAVIOURAL ADVERTISING

Developments in information and communication technologies (ICT) in recent years, in particular the emergence and expansion of Web 2.0, have led to users playing a more active role in the creation and sharing of content

DOI: 10.1515/wrlae-2015-0015

*Ph.D, Faculty of Law, Administration and Economics University of Wrocław, Poland, agata.jaroszek@uwr.edu.pl.

[1] Joanna Kulesza, 'International law challenges to location privacy protection' (2013) 3 (3) International Data Privacy Law.

[2] Richard C. Turkington, Anita L. Allen, *Privacy Law Cases and Materials* (American Casebook Series West Group 1999) 325.

than was the case in the traditional website model, whereby mainly passive access to content entirely controlled by the owner of the website was permitted.

Modern computer storage capabilities, more efficient analytical software, and widespread broadband connectivity of computer networks together allow permanent recording of information. These new uses of the World Wide Web have led to the development and evolution of new web-based communities and hosted services, such as social networking sites (e.g. Facebook, MySpace), video sharing sites (e.g. YouTube), wikis, and blogs, which have become very popular among young users, including young children[3].

Children have, of course, been targeted by the tactics and strategies of marketers ever since the early days of television; however, since the mid 1990s not only has the internet become a new medium for advertising practices aimed at children, but an increase in the collection of children's data has also been observed and verified by different studies in media communication. For decades scholars and privacy advocacy groups declare that the "long standing battle policy over issues such as violent content, indecency and advertising is likely to continue"[4].

The policy debate over children's advertising, in particular online behavioural advertising, is gaining in significance since it creates the risk of being able to precisely analyse children's conduct, which in turn carries the risk that persuasive marketing strategies, almost tailor-made to an individual child based on data relating to his or her behaviour, will be employed with the aim of having a direct impact on the choices made by child consumers[5].

What exactly, then, is online behavioural advertising (OBA)?[6] This is a special form of targeted advertising that entails tracking users' browsing activity on the internet and the building of profiles over time, which are later used to provide them with advertising matching their interests (e.g. to remember what's in their online basket[7], or to ensure security in online banking). According to McStay, it is a form of commercial solicitation that is intrinsically reliant on data deliberately or unintentionally provided by users,

---

[3] Web 2.0 – the concept that is used to describe new uses of the World Wide Web technology, see e.g. *What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software*, <http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html>, see also Joshua Stern, *Introduction to Web 2.0 Technologies* 1-2,< www.wlac.edu/online/documents/Blogging_v.02.pdf> accessed 12 November 2015.

[4] J. Alison Bryant (ed), *The Children's Television Community* (Routledge Communication Series 2006) 253.

[5] Blandína Šramová, 'Marketing and Media Communications Targeted to Children as Consumers' (2015) 191 Procedia - Social and Behavioral Sciences 1525.

[6] Also known as interested-based advertising.

[7] For example, basket analysis is said to be consumer oriented because it treats a discrete aspect of consumption behaviour. Julander (1992) provides other reasons for using basket analysis. Taking the bundle of items purchased on an occasion enables retailers to develop a richer picture of consumer behaviour. It can also provide insights into information relating to the effectiveness of store layout, the structure of demand, product range decisions and consumer behaviour. There are a number of other reasons for using this type of analysis. Such reasons include the relative ease of data gathering, the ability to relate purchase history to customer data (through loyalty card schemes), the timeliness of data and its modest cost. Such advantages lend themselves to attempts to classify consumers by examining the mix of products bought, see, Barry Davies, Stephen Worrall, 'Basket analysis: profiling British customers' (1998) 100 (2) British Food Journal 102 – 109.

and facilitates advertising takes the form of advertising based on analyzing and assessing the users' activities on the web. Furthermore, OBA involves the examination of communication and information as it passes through the gateways of internet service providers (ISP)[8]. The majority of these activities are accomplished through persistent identifiers such as IP addresses and cookies that can be linked to individuals.

An accurate description of how OBA works on a technological level is provided by S. Kumar[9]. According to her, OBA involves two types of targeting. First-party targeting is where user behaviour is tracked by means of a cookie on a specific website[10]. The data is kept by the website owner (or a company providing contractual services), and targeted ads are served up while a user is browsing the site. In such network advertising models a number of sites connect with each other to share the data about users' journeys across a specific network of sites[11].

The second type of targeted marketing is ISP-based behavioural targeted advertising. This involves advertisers placing software within the ISPs' networks, allowing them to intercept all users' browsing activity using "deep-packet inspection"[12], thereby putting each user into a "bucket" that broadly and anonymously categorises them and serves them ads based on which "bucket" they are in. Whilst this enhances the quality of the targeting (as it covers a broader range of sites), it is also more invasive than first-person or network targeting as it collects information on the user's entire web activity[13].

A good example of ISP-based behavioural targeted advertising is the case of the Phorm company[14]. In 2008, Phorm, US-based company, signed a contract with the United Kingdom's three largest ISPs[15] to use and install its advertising system. There were strong objections raised by privacy advocates about Phorm's ad tracking system, which involved the interception of all the web pages visited by customers of these ISPs and then engaged in scanning web pages for key words, including Google search results. The frequency of the key words were used to build a profile of each customer's interests to

---

[8] Andrew McStay, *The Mood of Information: A Critique of Online Behavioural Advertising* (Bloomsbury Publishing 2011) 2.

[9] Seetha Kumar, 'BBC Online and behavioural targeting' <http://www.bbc.co.uk/blogs/bbcinternet/2009/05/bbc_online_and_behavioral_targ.html> accessed 12 November 2015.

[10] A small text file used by many businesses to check the current status of a user and perform the choice the user wishes to exercise. These are essential to this function as well as identifying errors in its functionality. Cookies, which contain a randomised identifying number, are placed on a user's machine. The cookie then tracks websites visited and draws conclusions about a user's behaviour in order to target more relevant adverts.

[11] Kumar points out that the website's privacy policy should tell a user how to opt out if he/she does not want his/her user journey record used in this way. See Kumar (n 9).

[12] A term used to describe an advanced interception technology.

[13] Kumar (n 9).

[14] Phorm, formerly known as 121Media, is a digital technology company known for its contextual advertising software. Phorm is incorporated in Delaware but relocated to Singapore as Phorm Corporation (Singapore) Ltd in 2012 <https://en.wikipedia.org/wiki/Phorm> accessed 12 November 2015..

[15] BT, TalkTalk, and Virgin Media.

provide tailor-made advertising[16]. The criticism of the system was based on allegations that British ISPs were selling information about users on to a third party[17].

The Phorm's advertising system is a prominent example of the privacy implications of tracking users' conduct online; nevertheless, other online behavioural advertising practices that have likewise raised concerns among privacy advocates and consumer groups are also worthy of mention, such as:

a) web operators making access to online services (e.g. social network services' practices) conditional on the prior disclosure of personal details;

b) behavioural marketing practices that expose internet users' personal information to marketers, advertisers, and other third parties without users' knowledge, such as Facebook's "Sponsored Stories", which is a type of advertising that seeks to use images of teenagers in online advertising;[18]

c) websites such as Amazon, which "operates a site featuring products tantalizing to children, and then disclaims any responsibility for marketing to children by asserting in its privacy policy that it technically only sells products to adults"[19].

Article 29 of the Working Party gives an example of social networks where, as a rule, access to services offered is often subject to agreeing to different kinds of processing of personal data. The user may be required to consent to receiving behavioural advertising in order to register with a social network service without "further explanation", i.e. they are required to consent without being told exactly why or without being given alternative options. Some categories of users (such as teenagers) will agree to receive behavioural advertising simply in order to avoid the risk of being partially excluded from social interactions[20].

Another related problem identified in the studies, which concerns the need to provide special protection of children's data in digital form, is the issue of a commercial practice concerning website operators' privacy policies that may not be in full compliance with the existing rules, may not be clear about the purpose of collecting data from children in particular, may not be easily accessed, and, last but not least, may be written in language that is not easy to understand (e.g. complicated legalese), especially for younger children.

The problem of online behavioural advertising targeted at children could be discussed from at least three perspectives, i.e. a critical analysis of the European legal framework on advertising, consumer, and personal data

---

[16] Christopher Williams, 'BT and Phorm: how an online privacy scandal unfolded. The Crown Prosecution Service's decision not to prosecute BT and Phorm over their secret interception of internet traffic closes a chapter of Britain's biggest online privacy scandal' <http://www.telegraph.co.uk/technology/news/8438461/BT-and-Phorm-how-an-online-privacy-scandal-unfolded.html> accessed 12 November 2015..

[17] See 'Users offered ad tracking choice' < http://news.bbc.co.uk/2/hi/technology/7289481.stm> accessed 12 November 2015..

[18] See Brief of *Amicus Curiae* Electronic Privacy Information Center (Epic) in Support of Appellants Case No. 13-16918.

[19] Before the Federal Trade Commission Washington, DC In the Matter of Amazon.com, Inc. EPIC Complaint and Request for Injunction, Investigation and for Other Relief <https://epic.org/privacy/amazon/coppacomplaint.html>accessed 12 November 2015.

[20] Art. 29 Working Party Opinion 15/2011 on the definition of consent, 18.

protection may be conducted. A discussion of all of the issues involved is, however, beyond the scope of this paper.

The difficulty and complexity of privacy issues involved in using OBA lie within the potentially conflicting relationship between the economic interests of advertisers, on the one hand, and the fair treatment of the interests of internet users to ensure the protection of their personal data (including sensitive data such as that relating to health, finances) from unauthorized access or collection for unknown purposes, on the other. The remainder of this paper will primarily focus on providing an overview and analysis of existing as well as future policies and initiatives that address the potential privacy risks children might be exposed to while being targeted by OBA techniques.

II. PROTECTION OF CHILDREN'S PERSONAL DATA UNDER EU LAW

The European Union is committed to protect the rights of children, defined as anyone under the age of 18 under in the United Nations Convention on the Rights of the Child (UNCRC). The UNCRC reflects a balance between the rights and responsibilities of family members (i.e. parents, caregivers or guardians), on the one hand, and the recognition of the child as a human being with an evolving capacity to make decisions affecting her or his life, on the other. A comprehensive, holistic approach towards children's rights consists in interpreting the various rights of the Convention through general principles such as non-discrimination, the best interests of the child, and respect for the views of the child[21].

The UN Convention recognises the vulnerability of children in certain circumstances, but also their capacities and strengths as rights holders. This approach of affording special protection to children as enshrined under the UN Convention is also mirrored under Art. 24 of the Charter of Fundamental Rights of the European Union.

III. THE NOTION OF SPECIFIC PROTECTION OF A CHILD

The right to privacy of the child (as enshrined in the Article 16 UNCRC) becomes an integral part of the EU's fundamental rights policy under Art. 8 of the Charter, which is distinct from the right to respect for private and family life, home, and communications set out in Article 7 of the Charter. It derives from Article 8 of the European Convention on Human Rights (ECHR) and the case law of the European Court on Human Rights on the protection of privacy and private life, although the protection of personal data is not, as such, explicitly mentioned in the ECHR[22]. Interestingly, the European Economic and Social Committee, in its opinion published in 2012, expressed the view that the issue of advertising that targets children and

[21] Art. 24 Commentary of the Charter of Fundamental Rights of the European Union, EU Network of Independent Experts on Fundamental Rights, 209.

[22] T. Ojanen, substitute of M. Scheinin, Art. 8 Commentary of the Charter of Fundamental Rights of the European Union, EU Network of Independent Experts.

young people is, first and foremost, an issue of citizenship and the protection of fundamental rights[23].

Through its EU Agenda for the Rights of the Child adopted in 2011, the Commission aims at achieving a high level of protection of children in the digital space, including protection of their personal data, while fully upholding their right to access the internet for the benefit of their social and cultural development[24]. The need to strengthen the protection of children in the online environment is supported by the findings of various studies of children's online activities and the perception of risks. The Safer Internet for Children qualitative study that focussed on children aged 9–10 and 12–14 shows that children tend to underestimate risks linked to the use of the internet and minimise the consequences of their risky behaviour[25]. The OECD report finds that children do not have a developed ability to engage critically with aggressive online advertising practices and the impact of geo-localisation[26].

The OECD report also admits that worldwide legal measures related to protecting children against OBA are inconsistent as they governed by general rules of national data protection legislation and in some countries supplemented by self-regulatory principles for online behavioural advertising developed by advertising initiative groups or associations[27].

IV. THE GENERAL EUROPEAN LEGAL FRAMEWORK FOR OBA

In the European Union, data protection is regarded as a fundamental right under Article 8 of the Charter of the Fundamental Rights, and is, moreover, a constitutional freedom in many European countries. The general European legal framework is based on Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as well as the amended Directive 2002/58/EC[28] (known as the ePrivacy Directive) concerning the processing of personal data and the protection of privacy in the electronic communications sector that serves as the *lex specialis*. This means that the provisions of Directive 95/46/EC on issues such as the legal grounds for data processing, the principles regarding data quality, the data subject's rights (such as the right to access, erase, and object), confidentiality, and security of processing and international data transfers will be fully applicable, except for those provisions that are specifically addressed in the ePrivacy Directive[29].

---

[23] See the Opinion of the European Economic and Social Committee on *A framework for advertising aimed at young people and children* (own-initiative opinion).

[24] Commission, 'An EU Agenda for the Rights of the Child' COM (2011) 60 final.

[25] The Safer Internet for Children qualitative study <http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm> accessed 12 November 2015.

[26] OECD, 'The protection of children online: Risks faced by children online and policies to protect them', OECD Digital Economy Papers (2011) 179, OECD Publishing.

[27] ibid 33.

[28] As amended by Directive 2009/136/EC.

[29] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy

Under the general Directive 95/46/EC and the ePrivacy Directive 2002/58/EC, a child enjoys the same level of protection as an adult on issues such as, for example, the right to be informed about the purpose of processing data or the right to object to processing operations. The directive does not include any special provisions concerning protection of the personal data of children or exclusive safeguards for the online processing of data of children.

In the context of online behavioural advertising, it is essential to refer to Opinion 2/2010 on online behavioural advertising, where the Article 29 Working Party clarified the legal framework applicable to parties involved in such practices, i.e. ad network providers, publishers, and advertisers. This body has made a significant contribution to understanding among stakeholders and general audiences in this area by publishing material that provides clarity and guidelines for interpreting the existing European data protection law on the processing of children's personal data, especially in digital forms[30]. As noted by the Article 29 Working Party, online behavioural advertising techniques often entail the processing of personal data as defined by Article 2 of Directive 95/46/EC due to the following facts: a) behavioural advertising normally involves the collection of IP addresses and the processing of unique identifiers (through cookies) – cookies and respective scripts can be distinguished into ID-cookies, that is personal identifiable information, and as such they qualify as personal data; b) it involves the monitoring of user's activity online and, even more widely, the aggregation of personal information (a person's characteristics or behaviour) for a variety of purposes (e.g. to influence that particular person)[31].

Under the current framework, data processing operations are allowed upon the consent of the data subject[32] (under the ePrivacy Directive a data subject is defined as a user or subscriber), which serves as one of the main criteria for legitimate processing by a data controller[33].

---

and electronic communications) [2002] OJ L 201/37. Article 2 of the ePrivacy Directive says: "The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1".

Both directives were implemented as an enacted law in the Member States.

As to the scope of application of these two directives in the context of OBA, see explanations given in Opinion 2/2010 on online behavioural advertising. See also Opinion 16/2011 on 'the EASA/IAB Best Practice Recommendation on Online Behavioural Advertising'.

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

[30] See Article 29 Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, Article 29 Data Protection Working Party, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), WP 160, 11 February 2009, Opinion 2/2010 on online behavioural advertising, Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 01197/11/EN WP 187, 13 July 2011.

[31] Opinion 2/2010 para. 3, 8.

[32] A data subject - an identified or identifiable natural person, see art. 2 (a) of directive 95/46/EC.

[33] According to the Art. 2 (h) of Directive 95/46/EC, "the data subject's consent" shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. See Directive 95/46/EC Art. 7 (a) and 8 para. 2. (a); the latter refers to an explicit consent for special categories of processing. Art. 2 (d) "controller" shall mean the natural or legal person, public

As was confirmed by the Article 29 Working Party, in most cases cookies and IP addresses are to be considered personal data[34], therefore the application of a special provision, i.e. Article 5(3) of the ePrivacy Directive, which lays down protective measures for the confidentiality of communications in the concrete case of the use of cookies and similar devices, will be triggered[35]. From the perspective of website operators and their partner organisations, cookies are useful because they allow a website to recognise a user's device. Article 5(3) requires prior informed consent for the storage of or access to information stored on a user's terminal equipment. In other words, the requirement under Article 5(3) aims to prevent information being stored on people's computers and being used to recognise them via the device they are using without their knowledge and agreement.

On the one hand, Article 5(3) of Directive 2002/58/EC, as amended by Directive 2009/136/EC, has reinforced the protection of users of electronic communication networks and services by requiring informed consent before information is stored or accessed in the user's (or subscriber's) terminal device. On the other hand, Article 5(3) allows cookies to be exempted from the requirement of informed consent if they satisfy one of the following criteria: criterion A: the cookie is used "for the sole purpose of carrying out the transmission of a communication over an electronic communications network". Criterion B**:** the cookie is "strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service"[36]. Third-party cookies used for behavioural advertising are not exempted from consent, as was highlighted in detail by the Working Party in Opinion 2/2010 and Opinion16/2011. This requirement for consent naturally extends to all related third-party operational cookies used in advertising, including cookies used for the purpose of frequency capping, financial logging, ad affiliation, click fraud detection, research and market analysis, and product improvement and debugging, as none of these purposes can be considered to be related to a service or functionality of an information society service explicitly requested by the user, as required by criterion B.

To sum up, Opinion 2/2010 emphasises the importance of complying with the requirement to obtain a data subject's prior informed consent to engage in behavioural advertising as well as for the placement of cookies on the user's browser in general[37]. Insofar as children are concerned, the Article 29 Working Party recommends setting out additional requirements for such

---

authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

[34] This was also confirmed in its Opinion 1/2008 on data protection issues related to search engines, adopted on 4 April, 2008.

[35] Opinion 2/2010 on online behavioural advertising, para.3, 7.

[36] Article 29 Working Party Opinion 04/2012 on Cookie Consent Exemption.

[37] In this context, it is important to take into account the fact that for consent to be valid whatever the circumstances in which it is given, it must be freely given, specific, and constitute an informed indication of the data subject's wishes. Consent must be obtained before the personal data are collected, as a necessary measure to ensure that data subjects can fully appreciate that they are consenting and what they are consenting to. Furthermore, consent must be revocable see the literal wording of Article 5(3) of the "ePrivacy Directive", the Opinion 2/2010, pt 4.1.

consent to be valid, such as parents or other legal representatives also providing consent in particular cases. In addition to complying with applicable advertising legislation and standards, ad network providers would need to provide notice to parents about the collection and the use of children's information and obtain their consent before collecting and further using their information for the purposes of engaging in behavioural targeting of children. In light of the above, and also taking into account the vulnerability of children, the Article 29 Working Party places great emphasis on the importance of publishers and ad network providers engaged in behavioural advertising complying with the obligation to obtain data subjects' prior consent to engage in behavioural advertising[38], and is of the view that ad network providers should not exploit collected information on the interests of specific groups of users to foster further behavioural advertising or influencing children[39].

V. SELF-REGULATORY OBA INITIATIVES

This view corresponds to solutions proposed within self-regulatory initiatives such as the EU Framework for Online Behavioural Advertising adopted by the Interactive Advertising Bureau (IAB Europe) in 2011[40]. This framework creates obligations for any signatory company that self-certifies its compliance with the following principles and obligations:

- notice;
- user choice over online behavioural advertising;
- data security;
- sensitive segmentation;
- education;
- compliance and enforcement programmes
- review

Children are mentioned under the sensitive segmentation principle, which imposes an obligation on companies not to create segments for OBA purposes that are specifically designed to target children. Interestingly, for the purposes of this provision the framework defines "children" as people aged 12 and under. Under the same principle any company seeking to create or use such OBA segments relying on use of sensitive personal data as defined under Article 8.1 of Directive 95/46/EC will obtain a web user's explicit consent, in

[38] Opinion 2/2010, para 4.1, 13.

[39] Especially ones that would reveal sensitive data or initiatives of ad network providers consisting in offering access to interest categories that data subjects have been labelled with based on the cookie ID number. See e.g. Google's Interest-Based Advertising Interest-based advertising that enables advertisers to reach users based on their inferred interests and demographics (e.g. "sports enthusiasts"). It also allows advertisers to show ads based on a user's previous interactions with them, such as visits to advertiser websites <http://www.google.com/ads/preferences/html/about.html>accessed 12 November 2015. These new tools enable users not only to access the interest categories that related to them but also modify them and erase them. See Opinion 2/2010 para. 5.

[40] The Self Regulatory Principles for Online Behavioural Advertising have been developed by a cross-industry effort at European level, with EASA's (European Advertising Standards Alliance) Best Practice Recommendation on OBA building on the IAB Europe (Interactive Advertising Bureau Europe) OBA Framework.

accordance with applicable law, prior to engaging in OBA using that information.

Interestingly, almost identical principles were developed in 2009 in the USA that served as a template for developing a European counterpart framework for addressing OBA. The American Sensitive Data Principle also recognizes that certain data collected and used for online behavioural advertising purposes merits different treatment. Therefore, the protective measures set forth in the Children's Online Privacy Protection Act must be applied[41]. It is worth mentioning that the US 1998 Children's Online Privacy Protection Act (COPPA; effective April 21, 2000) directly protects the privacy of children under 13 years old on the internet. As the first law directly addressing privacy in cyberspace, the law has been heavily criticised, firstly for not having granted statutory protection to a child who is over 13 years old (the question of age limitation), and secondly for providing an exemption from compliance with statutory requirements where website operators have no actual knowledge that they are collecting the personal data of a child.

In 2011, the Federal Trade Commission (FTC) proposed to amend the Children's Online Privacy Protection Rule (the "COPPA Rule") that emanated from the requirements of the Children's Online Privacy Protection Act in order to respond to changes in online technology, including in the mobile marketplace[42].

Alongside the EU Framework for Online Behavioural Advertising, a cross-industry self-regulatory initiative was developed by leading European bodies to introduce pan-European standards to enhance transparency and user control for online behavioural advertising by launching[43]. A consumer-focused website and education portal (www.youronlinechoices.eu), available in all official EU and additional EEA languages, provides a mechanism for web users to exercise their choice with respect to the collection and use of data for online behavioural advertising purposes by one or more third parties, or links to a mechanism permitting user choice over online behavioural advertising. Their approach consists of an icon to be placed on each targeted ad, coupled with an information website that allows the user to switch off behaviourally targeted display ads from any participating company. This currently works by requiring opt-out cookies and is backed by an enforcement mechanism[44]. Consumers are allowed to exercise control over receiving targeted ads by using an opt-out tool provided by website operators.

It is worth stressing that the Article 29 Working Party, in its Opinion on the definition of consent, expressed a strong belief that the interests of children and other individuals lacking full legal capacity would be better protected if Directive 95/46/EC contained additional provisions that were

---

[41] In 2014 the US Framework was supplemented by Self-Regulatory Programme for Online Behavioral Advertising released by IAB and other US main participating associations to empower American consumers to manage their data <http://www.iab.com/news/self-regulatory-program-for-online-behavioral-advertising/>
accessed 12 November 2015.

[42] See 16 C.F.R. Part 312: Children's Online Privacy Protection Rule: Proposed Rule; Request for Comment on Proposal to Amend Rule to Respond to Changes in Online Technology <https://www.ftc.gov/policy/federal-register-notices/16-cfr-part-312-childrens-online-privacy-protection-rule-proposed>accessed 12 November 2015.

[43] Based upon IAB Europe's OBA Framework and EASA's BPR on OBA.

[44] < http://www.youronlinechoices.com/uk/your-ad-choices> accessed 12 November 2015..

specifically addressed to the collection and further processing of their data. Criticism of the directive for lacking some protective measures necessary for safeguarding legitimate processing in the digital networks resulted in the drafting of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) at the beginning of 2012[45]. The proposal's key changes include:

- easier access to personal data of individuals and transfer personal data from one service provider to another (right to data portability);

- more detailed information provided by data controller in the plain language about the purpose and duration of processing (transparency)**;**.

- a right to erasure of personal data and "to be forgotten", that will enable to require from a service provider to remove, without delay, personal data collected when that individual was a child;

- limits to the use of 'profiling', i.e. automated processing of personal data to assess personal aspects, such as performance at work, economic situation, health, personal preferences etc

- overreaching application of EU laws to service providers established in third countries (i.e. USA, China) who process personal data of EU citizens[46].

VI. NEW REQUIREMENTS FOR SPECIAL PROTECTION OF A CHILD UNDER THE PROPOSAL OF THE GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation draft proposal provides a new set of rules for the protection of personal data, having adopted the core legal principles laid out in the general Directive and following a technology-neutral approach to regulation of the issues in question. The Commission's commitment to support the need to provide specific protection to children is based on the fact that they may be less aware of risks, consequences, safeguards, and their rights in relation to the processing of personal data (Preamble 29). In addition, the proposal aims to introduce a measure that prohibits children's profiling through automated processing (Preamble 58). Secondly, the Commission aims at introducing a balancing test that weighs, on the one hand, the legitimate interests of a controller that may provide a legal basis for processing, provided that the interests or fundamental rights and freedoms of the child data subject are ensured, including the right to object, free of charge, to processing on grounds relating to their particular

[45] COM (2012) 11 final. The new legal framework for the protection of personal data in the EU consists also of a proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data that also highlights the protection of a child (see Art. 45 (2) of the draft directive COM/2012/010 final).

[46] Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses <http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en> accessed 12 November 2015..

situation; and the need to ensure transparency through the controller's obligation to explicitly inform the data subject of the legitimate interests pursued and his or her right to object, and to document these legitimate interests, on the other (Preamble 38).

The new proposed regulation advocates the transparency principle, which purports to ensure that, where processing is addressed specifically to a child, the controller's obligation is to provide any information and communication in clear and plain language that the child can easily understand (Preamble 46). The need for children to enjoy special protection is reflected under Art. 6 (1)f concerning the lawfulness of processing necessary for the purposes of the legitimate interests pursued by a controller[47]. Firstly, transparency has to be ensured, in particular where the data subject is a child. The requirement for information to be adapted to children in order to make it easier for them to understand what it means when their data are collected, thus meaning they are able to provide informed consent, is a positive step.

VII. PROCESSING OF CHILDREN'S PERSONAL DATA IN RELATION TO INFORMATION SOCIETY SERVICES

Secondly, Art. 8, which provides special protection for the processing of a child's personal data, sets out further conditions for the lawfulness of the processing of such data in relation to information society services offered directly to them. The concept of the protection of a child in an online environment adopted under the draft is already in operation in the United States' COPPA Rule. By analogy, data controllers in the European Union will be obliged to obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children under 13 years of age. Following the accountability principle, it should be left to the controller to make reasonable efforts to ensure it obtains verifiable consent, taking into consideration the available technology. Focus has now shifted to a revision of the COPPA Rule on proposing reliable methods of parent verification when consent is sought.

Critics of this provision object to its exclusion of the 14–17 age group, who are instead protected by general requirements (including the direct consent of a data subject) laid down in the draft regulation. Discussion of the importance and multidimensional character of this topic is beyond the scope of this paper, however[48]. The wording of the proposed provision raises concerns about the scope of the provision limited to information society services or situations where parental consent cannot be obtained, while it also fails to set out specific safeguards identifying data processing activities, such

[47] The draft provision excludes the legitimate interests of third parties to whom the data are disclosed.

[48] A critical analysis of the practical implications of the European Commission proposal under Art. 8 is presented in the article written by Lina Jasmontaite, Paul De Hert , 'The EU, children under 13 years and parental consent' (2015) 5 (1) International Data Privacy Law 20-33.

as behavioural advertising, where consent should not be a possible basis to legitimise the processing of personal data[49].

Moreover, the draft regulation does not refer to the issue of the obligation to use age verification mechanisms, as advocated by the Article 29 Working Group[50]. This is regrettable since they could be a possible solution for protecting children and young people from content that may be harmful to them or may prevent them from consenting to the processing of their data. The arguments against introducing age verification mechanisms point out that requiring users to go through an age verification process would lead to a distinct loss of personal privacy[51]. Moreover, at present there is no single technical solution for online age verification that does not infringe on other human rights and/or is not exposed to age falsification[52].

CONCLUSION

The issue of behavioural advertising and other marketing techniques that aim at profiling children is a difficult and complex one that requires the joint efforts of the ICT industry, policy makers, and privacy and consumers organizations, as well as parents, guardians, and children themselves, in order to create future privacy laws where the fundamental rights to freedom of expression and privacy protection outweigh the economic interests of the advertising industry and the monetization of information concerning an individual.

To summarize the discussed problems, it should be noted that, according to the Eurobarometer survey on Attitudes on Data Protection and Electronic Identity in the European Union, almost all Europeans believe that underage children should be specially protected from the collection and disclosure of personal data, and also that minors should be warned of the consequences of collecting and disclosing personal data[53]. Europeans' opinions are divided with respect to the circumstances under which police should have access to personal data. In contrast, almost everyone agrees that minors should be protected from and warned against the disclosure of

---

[49] The Article 29 Working Party The opinion 2/2010.

[50] Article 29 Working Party, Opinion 2/2010. The Working Party proposed to develop solutions for individuals lacking legal capacity that will specifically address the following issues:

i. Clarifications as to the circumstances in which consent is required from parents or representatives of an incapable individual, including the age threshold below which such consent would be mandatory.

ii. Laying down the obligation to use age verification mechanisms, which may vary depending on circumstances such as the age of children, the type of processing, whether particularly risky, and whether the information will be kept by the data controller or made available to third parties;

[51] 16 CFR Part 312 RIN 3084–AB20 Children's Online Privacy Protection Rule.

[52] Recommendation CM/Rec (2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CM%20Rec%282012%294_En_Social%20networking%20services.pdf>accessed 12 November 2015.

[53] Special Eurobarometer 359

personal data, and is in favour of the special protection of genetic data[54]. With emerging technologies such as the "internet of things" and cloud-based services, the potential for future legal, technological, and moral controversies is great.

The attitude of the Europeans surveyed reflects the European Commission's policy as articulated in the Communication: European Strategy for a better Internet for Children document[55], which aims at developing protective measures by employing a combination of regulatory, self-regulatory, and educational tools in order to establish standards for creative and secure usage of internet services by children.

So far the solutions offered are not fully convincing; see the methods of obtaining consent or establishing the age threshold for children who can be targeted for OBA purposes, for example. The main facilitator of behavioural advertising is cookies. The risk to data protection comes from the action of processing the data rather than the simple storage of information contained within the cookie, however. The recent move to disseminate opt-in policies for cookies is welcome, though the issue of effectiveness of obtaining a user's consent under Art. 5(3) of the ePrivacy Directive remains controversial. As was observed by Riefa and Markou, internet users (in my view, especially children) need "control tools at the data collection stage" that could be developed according to the level of a child's evolving capacity to take decisions affecting her or his life (private sphere). Moreover, other tools, such as "appropriate advert labelling [i.e. an icon appearing on advertisements on websites] provided or the use of compulsory default browser settings that block tracking cookies" could play an important role in ensuring compliance with better protection standards set by relevant consumer and unfair practices legislation[56].

[54] ibid 206.
[55] COM (2012) 196 final.
[56] See an excellent contribution to discussion on the EU cookie policy and risks involved in OBA: Christine Riefa, Christiana Markou, 'Online marketing: advertisers know you are a dog on the Internet!' in Andrej Savin, Jan Trzaskowski (eds), *Research Handbook on EU Internet Law* (Edward Elgar Publishing 2014) 383-410.