

5 CMET (2018) 40

Behavioural Dvertising and Data Protection

by

Pallavi Khanna¹

INTRODUCTION

Mass advertisements online are gradually paving the way for targeted or behavioural advertising which is tailored to meet the preferences, needs, interests and expectations of the internet users. When users browse the internet, they come across a number of advertisements that are linked to their earlier surfing activity such as websites, online buys, keywords, etc. Advertisements are framed to suit the previous behaviour of the users or characteristics which have been attributed to them by their profiling. The behavioural tracking is supportive of a new kind of internet economy where the prime currency is the data of users.¹ The advancement in technologies has been significant and this has helped track consumer behaviour.

As the internet develops and becomes an indispensable element of the daily lives of a number of people, a number of advertising agencies invest time and money to increase revenues from the internet economy. A significant feature of this investment is the shift to targeted advertising which is tailored to the interest of internet users.² The marketing industry also seeks to benefit from the advertising campaign by enhanced revenues.³ Hence, advertisers must find efficient means to gain more revenue in the form of profits for all advertisements they put on the internet. There are higher chances of users opting for advertisements connected to their preferences and tastes over the ones which are irrelevant for them.

Through the course of this paper, the author seeks to analyse how behavioural advertising takes place, what the arguments in support of and against it are, the privacy concerns raised with regard to this issue, how the legal framework attempts to safeguard the interest of the consumers in this regard and what steps can be taken to overcome the threats emerging from targeted



advertising. The hypothesis that would be guiding the author is- "Behavioural tracking as part of profiling for online behavioural advertising (hereinafter OBA) constitutes a threat to the Internet user's rights to privacy and data protection and that the current counter - tracking initiatives are insufficient to protect users from that threat."

HOW DOES PROFILING AND TRACKING TAKE PLACE?

Apart from cookies, other technologies such as web bugs, html, etc. trace IDs and other personal information to use it for profiling. Behavioural tracking is designed in a manner that makes it useful for surveillance and monitoring through which consumers can be linked to personal data such as names, credit card details, etc. The foremost problem with tracking is that the users are mostly unaware that they are being tracked since it is done in an invisible way and requires knowledge beyond that of an average internet user in order to realise and prevent the same. Thus, the question of tracking being infringing to the private lives of people may be raised. There is a debate on the users' right to consent or refuse tracking as well. Surveys indicate that most of the users would have abandoned tailored advertising if they had knowledge of the

practices employed by the advertising companies for obtaining their data.⁴ Through the recent awareness campaign regarding tracking, certain consent mechanism such as 'do not track' have been introduced where users can set their preferences on tracking to be sent to advertising companies. Apart from this blocking tools and tracking protection initiatives also seek to mitigate effects of breach on the privacy of users.

OBA is a kind of targeted advertising through which companies track the online actions of its users so as to focus on them for the purpose of digital advertising which is directed at specified interests.⁵ This type of advertising is based on observations of the online behaviour of the internet users. OBA seeks to make advertising more appealing to the users by making them tailored to meet their preferences so that it is in accordance with their online habits. In pursuance of this, detailed profiles of users are built based on their behaviour as is evident from their online activities.

As per the Federal Trade Commission of the US, OBA entails consumers, online activities, tracking of the activities, advertising suiting their online activities.⁶ Article 29 Working Party (hereinafter WP) also noted that unlike



contextual and segmented advertising, OBA gives a detailed image of the subjects' online life, links of websites visited and even the length of time articles were viewed.⁷ Online advertising involves parties in addition to the advertiser, advertising company and website-provider or publisher. Advertisements are a source of profit for advertisers and website-providers keep space for advertisements so entities can advertise their products effectively. The advertising network acts as the connecting link between the website providers and advertisers. This multiplicity of stakeholders shows that there are plural interests behind OBA which is based on profiling and tracking. Profiling enables ad networks to know what content would be of interest to the user since valuable information is processed to make the ads more appealing for the users, it allows personalisation of advertisements to meet the interest of users.

WHAT IS PROFILING AND TRACKING?

OBA is the process of following the online actions of the users, tracing their habits and retaining information when the internet is being used.⁸ A detailed user profile usually consists of purchases, movies watched, hobbies, age, location and other pieces of information which are relevant for advertisers.

Tracking technologies enable automatic storage of data. The files, add-ons and analytics are some of the tracking technologies which are used to follow the users of the internet in order to collect data about their online behaviour. Tracking may be done on one web portal i.e. the one providing the tracking technology on its website or on several other portals where the tracking technologies are used to gather data about the browsing activity of the user across different websites. The latter is more useful for profiling since it provides the collecting entity a wide range of data. It is also the tracking system which is most invisible and hard to detect.

Cookies, web bugs, GIFs, HTML, web storage, browser fingerprinting, social network plug-ins, spyware are the popular tracking mechanisms. The tracking technologies have different characteristics but perform essentially the same function of obtaining information and identifying users with the help of demographic data, purchase interests, etc. though the information is anonymized and doesn't directly connect to a user, it can be used to infer their profile at some point in time. It is interesting to note that most of the tracking technologies are persistent and do not have an expiration

date so if the users are not aware of their existence and do not delete them then they will be continued to be tracked indefinitely, thus when a user believes she is not being tracked, even then, she might be tracked and profiled. Since most of these technologies are not visible to users, such as web beacons, they see

 Page: 43


them only on searching for it. It is often not clear who is the controller of the tracking technology, it could be the website provider or a third party who is unknown to the user such as an advertising network which has an established relation with website providers.

THE USER'S PERSPECTIVE

Surveys have revealed that users feel that behaviour advertising contravenes the consumer expectations and is viewed as a privacy harm.⁹ Users also feel that they would be more cautious if they knew that advertisers were using their activities to gather data.¹⁰ It is evident that people do not understand when and how tracking technologies work and transfer data. This limited awareness results in restricted abilities because internet users do not know how to enact an online privacy system. There is also a lack of control over the data collected and how it is displayed on public platforms.¹¹ Users, on one hand, may find OBA to be unpleasant due to the pop-up nature of advertisements hindering their browsing experience or on the other hand, find it interesting because of the content. However, it is important to note that this is in the absence of knowledge of how OBA works and the reaction of those in the knowledge of how it works is scary.¹² Thus, the lack of awareness makes it impossible for users to protect themselves from undesirable tracking since it is hard to opt out of things you are not aware of.¹³

Profiles are generated by employing technologies to gather data by tracking and other technologies. The more the industry of digital marketing expands, the more advanced the tracking technologies become. OBA is a booming business running with the support of a number of stakeholders in the industry.

In the following section the author seeks to discuss the legal implications of tracking, with a focus on the fundamental right to privacy, data protection and its implications on the capability of the user to accept or reject behavioural tracking.

 Page: 44

LAW, PRIVACY AND TARGETED ADVERTISING

Profiling is not viewed as an illegal activity. In fact, even the Council of Europe understands its benefits for users, society and the economy since it leads to improved market segmentations by facilitating better services that meet the demands of customers. However, the inherent aspects of profiling do favour practices which are illegal and in violation of rights of individuals.¹⁴

The right of respect for private lives and protection of data are fundamental rights which the Charter of the European Union protects. Both these rights are significant for the European citizen. The right to privacy was first protected in the European Convention of Human Rights(ECHR). Although the Article 8 of the ECHR did not mention the word 'privacy', it was encompassed in the notion of right to private life.

The Convention 108, which deals with protection of personal data of individuals, was adopted by the Council of Europe for developing the right to privacy in Europe.¹⁵ Article 16 of the Treaty on Functioning of European Union also provides that everyone has the right of protecting personal data concerning them.¹⁶ Moreover, after the European Union Charter of Fundamental Rights, data protection has become a fundamental right. In fact, the Charter recognises the right as distinct from the right to privacy which is prescribed under Article 7. The Charter bases this protection subject to certain principles such as the fair processing principle, using for specified processes, legitimate basis to process personal data, based on consent, rights of data subject for accessing and rectifying data, etc. The Directives on Data Protection and e-Privacy along with legal instruments supporting the right are part of the framework of data protection in Europe. Directive 95/46/EC¹⁷ gives a protective framework to consumers for regulating the basis of processing data legitimately and for establishing rights and duties of parties involved. Keeping in mind the changing regulatory needs due to emerging technologies, the 2002/58/EC directive sought to deal with a number of issues arising in electronic communications.¹⁸

Since there is no concrete definition of the term privacy, the ECHR has interpreted Article 8 broadly and has noted that the term covers not only the physical and mental integrity but also the social identity of an individual.¹⁹




Information stored on the terminal equipment of electronic communications is part of the private lives of the consumers²⁰ and it has also been stated that information gathered by surveillance of the personal use of internet will be protected by Article 8 of the ECHR.²¹ The right to privacy can subside when the interference in private domain is based on legal reasons, is in pursuance of a legitimate goal and is proportionate. Hence, if the interference doesn't comply with this criterion, then it is not a justified and the right to privacy of users is violated. Since tracking is invisible to users, many doubts have been cast on its legitimacy though per se profiling is not prohibited.²² When the gathering of information is for preventing disorders, protect health and morals or for safeguarding rights and liberties, it is legitimate since the purpose is relevant to the act. However, OBA purposes become so general that it is hard to ascertain the specific purpose of intrusion and hence hard to justify. Thus legitimacy has to be judged according to the facts of each case. The need for proportionality implies that when faced with a choice, a less burdensome solution for the user must be selected so that disadvantages are not greater than the aims pursued.²³ In the case of OBA, more relevant and interesting advertisements are received in exchange of private information.

Tracking also threatens self-determination of information which essentially relates to an individual's control over his personal data and relates to enhanced participation of the user in processing her personal information.²⁴ In case of OBA, third parties collect information, often without the user's knowledge and consent in order to create profiles.²⁵ The user has certain rights such as the right to object to direct marketing, rectify inaccuracies in data, etc., however no user control over the profile data is present.²⁶

Data collected by tracking technologies often falls under the definition of personal data as per Article 2(a) of the Data Protection Directive. Addresses, phone numbers, etc. are seen as personal data. Even information regarding hobbies and working

conditions is viewed as personal data.²⁷ This enables trackers to identify subjects even if the data is anonymous. Article 29 WP

 Page: 46


also notes that detailed user profiles are made up with a lot of data that can be called personal in nature.²⁸

Directive 2002/58/EC also has certain provisions for electronic communications and Article 5(3) specifically makes a reference to cookies and other kinds of identifying technology. As per this provision, the user needs protection in the storing access of information stored which the tracking technologies try to attack.²⁹

Moreover, personal data can be liberally interpreted because of the use of the term 'information'. This provision safeguards interests of the subscribers of public services and also users who have not entered into contractual agreement with the telecom providers.³⁰ An indicator of free consent is the ability of the user to withdraw that consent without any negative implications.³¹ Hence the consent must be specific and informed when it's about access and storage of information. This implies that the user must make the choice consciously after being given information enabling him to decide such as what information will be gathered, what use will it be put to, till when the information will be stored, etc. The mode of obtaining consent must be user friendly and precede the collection of data.

Article 5(3) also puts forth the opt-in mechanism for identifying technologies when they store or access information which is already stored by the user. The user must provide her consent for this function and must show an active choice in order to show her preference. The choice should be given freely and must be specific and informed indicator of the wishes of the user such as ticking a box on websites. However, the provision has been misinterpreted and a notice on websites conveying that visiting the website amounts to user's consent does not amounts to making an active choice but only implies one which is not what the article seeks to achieve. Moreover, the information provided in the notice is also not sufficient to facilitate an informed choice. There is no way for approving the notice or monitoring how the information is used, as there is no compliance.³² Article 10 of the Data Protection Directive obligates the data controller to give users information about the identity of controller, purpose of use, right of accessing and modifying information, etc. It is unlikely that trackers who work on making their technology invisible will disclose their identity so as to comply with the Data Protection Directive.

Tracking technologies installed by third parties such as advertising networks having no relation with a user, are more likely to violate the right of

 Page: 47

data protection of users because the definition in Article 29 WP is interpreted in favour of third parties since they are difficult to locate and it is hard to establish consent requirements on third parties since the user doesn't interact with them.³³

The European Commission has proposed a General Data Protection Regulation (hereinafter GDPR) for overcoming the problems in the legal framework concerning data protection currently existing. The regulation has stringent provisions to regulate tracking technologies. By including IP addresses and cookies in the ambit of personal

data, the scope for regulating tracking has widened since it can be used to identify the data subjects.³⁴ Thus, the new regulations prescribe the conditions under which profiling and tracking is allowed and methods to protect against illegal activities by creating a solid basis of legal certainty. The regulation further mandates that when profiling results in legal implications regarding the subject's interests, rights and freedoms, the profiling will be allowed only when the law expressly authorises it by virtue of the consent of the subject or in furtherance of a contract.

The European Union (hereinafter EU) legislations are geographically restricted in scope to users or controllers in the EU, hence non-EU entities are not subject to the requirements.³⁵ There is also inadequate capacity in terms of resources and staff in the data protection authorities.³⁶ However, GDPR seeks to overcome these deficiencies by proposing capacity building, more jurisdiction, clearer consent requirements and introducing the right to be forgotten.³⁷

IS THE CRITICISM OF OBA JUSTIFIED?

Those opposing regulation of tracking argue that there is nothing to hide when one engages in online activities and therefore, privacy concerns are unnecessary.³⁸ However, the author opines that this is a misinterpretation of the right to privacy and confusing it with secrecy. As a fundamental right the individual must have autonomy over what they share. Apart from this, the proponents of the argument that some users enjoy targeted advertising tend to forget



that the debate is not about prohibiting but allowing the right to choose OBA or reject it if one wishes to. It is also said that the interest should be kept free from regulations so that the profit of marketers is not hindered by interference. While the economic benefits arising from this cannot be ignored, the author opines that the freedom of advertisers must be balanced with the individuals' fundamental right of privacy since rejecting OBA still leaves open other avenues of profits from contextual and regular online advertising. Moreover, refraining from showing targeted advertising to those who don't wish to see it does not imply that online advertisements don't exist. It is even argued that tracking and profiling don't harm rights and only when the accessed information is put to any use that the problems arise.³⁹

There are a number of counter tracking measures such as tracking protection lists which bar specific tracking technologies. They are also called blocking tools and afford the user with some amount of control over the information it wishes to disclose and to whom.⁴⁰ However, this requires awareness of tracking to be successful. Apart from this the private browsing modes and self-regulation also function as a counter tracking measure.⁴¹ The European Advertising Standards Alliance issues recommendations on best practices for OBA to advice on regulating advertisements by enabling user choice over their information by mechanisms such as opt-out systems.⁴² Though a detailed examination of the counter tracking measures is outside the scope of this paper, it can be said that the awareness of users and hence their notification and consent are significant aspects of respecting privacy. It is apparent that the initiatives are insufficient to address the issue of violation of privacy by behavioural tracking.

CONCLUSION

OBA forms a part of the everyday lives of users online, the marketing methods are now targeted and hence more beneficial since purchasing chances are higher when presented with something the eye is looking for. Though some enjoy the customised experience because of the ease and comfort of obtaining new information about

developments in latest trends, deals and offers along with saving time, this comes at the cost of our personal lives. The non-transparency of tracking and potential misuse of the information pose a serious threat since fast paced sophistication of tracking technologies is not

 Page: 49

accompanied by a similar increase in the knowledge of users about threats to their privacy. Thus, it is seen that behavioural tracking violates the fundamental right of privacy and data protection. To resolve this, express notification, adequate information, universal protection, in-built privacy safeguards, express consent, standardised opt-in requirements are needed. There must be privacy safeguards in the design of products and services right from the inception by accounting for threats from the beginning and developing applications which can fight the emerging threats of data breach. Initiatives such as the 'Do not track' must be made more popular as they will be useful in enhancing participation to promote privacy of users. Apart from this, encryption and anonymisers also give an easy way to govern use of personal data. The current legal framework though not sound-proof is sought to be made more effective with the GDPR. The recognition of pseudo anonymized data that can trace individuals and establish connection as personal data is a welcome step by the WP. The compliance with respect to consent requirements needs to be strengthened further. Tracking technologies must be regulated on the basis of their role and purpose. Having an expiration time for tracking technologies is also helpful so that users have more timely occasions to review their consent and have better control over their data. Obligations of entities who are in charge of the tracking technologies must also be clearly stipulated to ensure accountability. Stringent enforcement mechanisms by effective penalties and greater resources and personnel training is also needed. It is thus concluded that tracking is privacy invasive and the benefits are not a good trade-off for the disclosures made, however, an environment where privacy and targeted advertising can coexist is feasible if proper measures are undertaken.

* Independent Legal Practitioner, High Court of Delhi.

¹ Electronic Privacy Information Center and Privacy International London, *Privacy and Human Rights: An International Survey of Privacy Laws and Development* (Electronic Privacy Information Centre 2005) 112.

² Council Opinion 2/2010/EC of 22 June 2010 on online behavioural advertising 00909/10/EN WP 171 (Working Party Opinion).

³ Katerina Eva Matsa and others, 'Digital Advertising and News: Who Advertises on News Sites and How Much Those Ads are Targeted?' (Pew Research Center, 13 February 2012) <http://www.journalism.org/analysis_report/digital_advertising_and_news/> accessed 30 September 2017.

⁴ Joseph Turow and others, 'Americans Reject Tailored Advertising and Three Activities that Enable It' (2009) <<http://dx.doi.org/10.2139/ssrn.1478214>> accessed 3 November 2017.

⁵ Dominique Shelton, 'Online Behavioral Advertising Tracking Users: Gold Mine or Land Mine?' (2012) 5(1) *Landslide* 26.

⁶ Federal Trade Commission, 'FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting, and Technology' (Federal Trade Commission 2009) 8."

⁷ Working Party Opinion (n 2).

⁸ Peter Eckersley, 'What Does the 'Track' in 'Do Not Track Mean'?' (*Electronic Frontier Foundation*, 19 February 2011) <www.eff.org/deeplinks/2011/02/what-does-track-do-not-track-mean> accessed 1 October 2017.

⁹ Turow (n 4).

¹⁰ A McDonald and Lorrie Faith Cranor, *'Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising'* 2010 TPRC 201."

¹¹ Joshua Gomez, Travis Pinnick and Ashkan Soltani, *'Know Privacy'* (UC Berkley School of Information 10 October 2009) <<http://escholarship.org/uc/item/9ss1m46b>> accessed 12 October 2017.

¹² Lorrie F. Cranor, *'Can Users Control Online Behavioral Advertising Effectively?'*, [2012] 10 IEEE Security & Privacy 93.

¹³ Wesley Gee, *'Internet Tracking: Stalking or a Necessary Tool for Keeping the Internet Free?'* (2011) 20/1 CommLaw Conspectus <<https://scholarship.law.edu/commlaw/vol20/iss1/9>> accessed 15 October 2017.

¹⁴ Committee of Ministers, Council of Europe, Recommendation to Member States on the Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling, adopted on 23 November 2010 CM/Rec (2010)13.

¹⁵ Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [1981] ETS No. 108.

¹⁶ Treaty on the Functioning of the European Union [2012] OJ C326/47.

¹⁷ Council Directive 95/46/EC 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 L281/31.

¹⁸ Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37 (Directive on Privacy and Electronic Communications).

¹⁹ *Pretty v. United Kingdom*, (2346/02) 2002 ECHR 423.

²⁰ Y. Poullet, *'Terminal Equipment as a Virtual Home?'* in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer 2010).

²¹ *Copland v. United Kingdom* (62617/00) 2007 ECHR 253."

²² RE Leenes, *'Code and Privacy, or How technology is Slowly Eroding Privacy'* in Egbert Dommering and Lodewijk Asscher (eds), *Coding Regulation: Essays on the Normative Role of Information Technology* (TMC Asser Press 2005) 10.

²³ CB Tranberg, *'Proportionality and Data Protection in the Case Law of the European Court of Justice'* (2011) 1 (4) International Data Privacy Law 239.

²⁴ Arnold Roosendaal, *'We Are All connected to Facebook...by Facebook!'* in R. Leenes and others (eds), *European Data Protection: In Good Health?* (Springer 2013).

²⁵ MR Calo, *'Digital Market Manipulation'* (2013) 81 The George Washington Law Review 32.

²⁶ Brendan V Alsenoy, Eleni Kosta and Jos Dumortier, *'Privacy Notices v. Informational Self-Determination Minding the Gap'* (2014) 28/2 International Review of Law, Computer and Technology <www.tandfonline.com/doi/pdf/10.1080/13600869.2013.812594> accessed 1 November 2017.

²⁷ Council Directive 95/46/EC of 23 November 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

²⁸ Working Party Opinion (n 2).

²⁹ Directive on Privacy and Electronic Communications (n 23).

³⁰ E. Kosta, *Consent in European Data Protection Law* (Kluwer Academic Publishers 2013) 277.

³¹ Article 29 Data Protection Working Party, *'Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies'* (Adopted 2 October 2013) WP 208 3 (Working Party Document).

³² Working Party Document.

³³ Working Party Opinion (n 2).

³⁴ Council Opinion 4/2007/EC of 20 June 2007 on the Concept of Personal Data 01248/07/EN WP 136.

³⁵ Article 29 Data Protection Working Party, Working Document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites (Adopted 30 May 2002 5035/01/EN/Final WP 56).

³⁶ P De Hert and V Papakonstantinou, 'The Proposed Data Protection Regulation Replacing Directive' "95/46/EC: A Sound System for the Protection of Individuals' (2012) 28 Computer Law and Security Review 138.

³⁷ Article 29 Data Protection Working Party, Working Party on Police and Justice, The Future of Privacy, Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (Adopted 1 December 2009) 02356/09/EN WP 168.

³⁸ D. Solove, 'I've Got Nothing to Hide and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review 745.

³⁹ BJ Koops, 'Some Reflections on Profiling, Power Shifts and Protection Paradigms' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer 2008) 328.

⁴⁰ Kate Kaye, 'Mozilla and Stanford Pitch New Cookie Blocking Approach' (*AdAge India*, 19 June 2013) <<http://adage.com/article/dataworks/mozilla-stanford-pitch-cookie-blockingapproach/242553>> accessed 25 October 2017."

⁴¹ Gaurav Aggarwal, Elie Bursztein and Dan Boneh, 'An Analysis of Private Browsing Modes in Modern Browsers' (USENIX Security Symposium, August 2010) 79.

⁴² Oliver Gray and Angela Mills Wade, *Best Practice Recommendation on Online Behavioural Advertising* (EASA 2011) 9."

Disclaimer: While every effort is made to avoid any mistake or omission, this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification is being circulated on the condition and understanding that the publisher would not be liable in any manner by reason of any mistake or omission or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification. All disputes will be subject exclusively to jurisdiction of courts, tribunals and forums at Lucknow only. The authenticity of this text must be verified from the original source.