11-30-2022

Implication of Personalized Advertising on Personal Data: A Legal Analysis of the EU General Data Protection Regulation

Noor Ashikin Basarudin

Ridwan Adetunji Raji
Zayed University

Available Online at www.e-iph.co.uk
Indexed in Clarivate Analytics WoS, and ScienceOPEN

E-B Environment - Behaviour Proceedings Journal

AQoL2022Putrajaya
https://www.amerabra.org

e-IPH e-International Publishing House Ltd., United Kingdom

06th ABRA International Conference on Quality of Life
Double Tree by Hilton Putrajaya Lakeside, Putrajaya, Malaysia, 21-22 Nov 2022

Implication of Personalised Advertising on Personal Data: A legal analysis of the Eu General Data Protection Regulation

Noor Ashikin Basarudin[1*], Ridwan Adetunji Raji[2]

[1] Faculty of Law, Universiti Teknologi MARA Cawangan Pulau Pinang, Permatang Pauh Campus, 13500 Pulau Pinang, Malaysia
(* Corresponding Author)
[2] College of Communication and Media Sciences, Zayed University, Abu Dhabi, United Arab Emirates

Email of All Authors: noornshikin@uitm.edu.my, ridwan.raji@zu.ac.ae
Tel: +60133568206, +971504497886

Abstract
The accelerating emergence of personalised advertising is mostly driven by data. Accordingly, algorithmic profiling has become a constant experience for every online user in predicting preference and interest. The profiling process raises several issues of human privacy and personal data invasion. Therefore, this study adopts the doctrinal legal method through the analysis of International Instruments and the European Union General Data Protection Regulation as legal avenue to safeguard and protect online activities of the data subjects. The findings of this paper discuss the main principles to be observed by the data controller in ensuring the legality of personal data profiling. This paper suggests the profiling process to be design-based security due to unavailability of system procedure to human knowledge.

Keywords: Personalised Advertising; Algorithmic Targeting; Personal Data Profiling; EU General Data Protection Regulation

DOI: https://doi.org/10.21834/ebpj.v7i22.4160

1.0 Introduction

At this point, the global advertising industry is almost entirely algorithmic or programmatic. Indeed, the sophistication of the targeting and profiling mechanisms in personalised advertising are miles ahead of the traditional or early online advertising targeting techniques. In the early online advertising targeting approach, audiences are segmented mainly based on their demographics and locations, akin to the approach used for traditional ad mediums. However, the emergence of algorithms in adverting has unlocked unlimited access to various types of digital users' information that is now used for different types of targeting and retargeting models (Goldfarb, 2014; Kant, 2021). For example, in the name of personalised ad on google, the list of users' interests and activities that are tracked, listed, and used for ad customisation settings range from digital activities and data related to personal, family, relationship, financial, location, education, entertainment, relaxation, and platform-usage, to mention but very few.

eISSN: 2398-4287 © 2022. The Authors. Published for AMER ABRA cE-Bs by e-International Publishing House, Ltd., UK. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/). Peer–review under responsibility of AMER (Association of Malaysian Environment-Behaviour Researchers), ABRA (Association of Behavioural Researchers on Asians/Africans/Arabians) and cE-Bs (Centre for Environment-Behaviour Studies), Faculty of Architecture, Planning & Surveying, Universiti Teknologi MARA, Malaysia.
DOI: https://doi.org/10.21834/ebpj.v7i22.4160

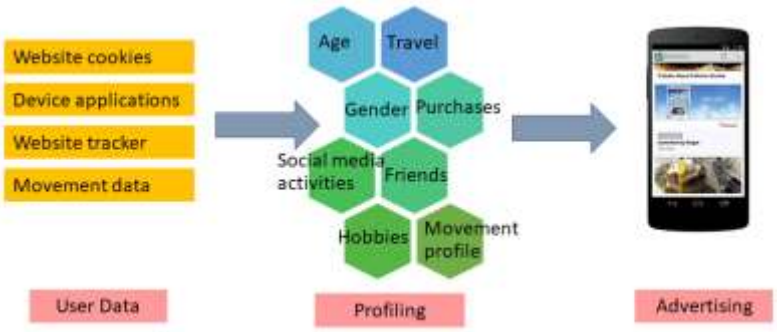

Fig. 1: User Profile Construction for Personalised Advertising
(Source: Author's Illustration)

The process illustrated in Fig. 1 begins with the collection of identified and identifiable of individuals information across the internet including demographic information, (e.g., name, age, country, education level), and the individuals' interests or preferences, respectively. The collection stage of user data is basically through website cookies, history of movement data, usage of device applications and website tracker. The next process involves the stage of identifying and targeting specific customer segments. However, not all digitally available information on the trillion pages of a website will be the target as some of them prevent the search engine from crawling and there could be a website that has poor reputation such as illegal ones. The information will be segmented and profiled according to the interest of a group of people through the algorithmic process of predictive analytics. Finally, specific online users will be fed with advertisements related to their interests and needs.

The moral ground for advertisers is that the more customised or personalised ads are, the more accurate, timely, and cost-effective brand information consumers get. Additionally, personalised ad content is presented to the audience as answers, solutions, or discoveries to their search queries, algorithmically tagged interests, etc. (Faggella, 2018). Hence, consumers are believed to benefit from algorithmic profiling as much as data aggregators and advertisers, as it reduces the cost and time of processing, searching, and buying on digital platforms.

However, barring the economic, commercial, experiential, and usability values of personalised advertising, However, barring the economic, commercial, experiential, and usability values of personalised advertising, some of the critical issues need to ponder particularly on its possibility in violating consumer privacy. Issues of privacy in personalised advertising is still in their infancy as a majority of the legal concern in advertising topics have dealt with the content itself either offensive (Hazelwood et al., 2018), sensitive or manipulative and its appropriateness to specialised audiences including children, adolescents and senior citizens (Noel et al., 2017). Therefore, this study aims at analysing the issue of privacy violations in personalised advertising and how the existing laws protect online users from data manipulation.

The algorithmic targeting profiling process is invisible to the eyes as no one would be aware of what types of data are gathered, and how it is inferred and disseminated. Moreover, a highly personalised and targeted online advertisement may lead to neurological undue influence and manipulations (Zuboff, 2019) to target the unconscious desires of consumers and potentially affecting their decision- making (Lenca & Andorno, 2017). In addition, the targeting and retargeting process in personalised advertising may suggest a fake testimonial and proliferation of click fraud. This type of manipulative action in advertising is difficult to prove in the court of law, hence, needs regulation to prevent from the initial process of data collection.

There are debates about the prohibition of targeted advertising based on pervasive tracking to prevent the misuse of personal data. Current challenges in personalised advertising are not on the 'targeted ads' but rather the issue of 'tracking-based ads' known as the behavioural and inferred data. It raises the question of consent considering the tracking and profiling of minors as the implementation of the consent requirement of age verification seems impossible across all internet services.

Furthermore, the existing Malaysia Personal Data Protection Act 2010 (PDPA 2010) approach is based on self-regulation when conducting personalised advertising including an expectation that any company collecting or processing consumers' private information should provide reasonable security for that information. This flexible approach invites the misuse of personal data as some specialised third parties collect consumers' personal information to be sold to other companies definitely without the customer's consent. For instance, data processor companies such as Google and Facebook have sourced consumers' data through selling hyper-targeted advertising based on algorithmically mining.

2.0 Literature Review

Algorithmic profiling or targeting is an automated process of tracking, mining, and using personal information to predict cyber users' preferences based on statistical inferences and evaluations (Blass, 2019). With the help of machine learning technologies and algorithms, advertisers deploy different targeting techniques, including contextual and behavioural targeting, to ensure accurate personalisation, customisation, and efficient contextualisation (Goldfarb, 2014).

Information gathered will be classified according to identified features to offer personalised goods and services based on geographical location and viewing habits. For instance, contextual targeting enables the display of personalised ad content that aligns with the media

vehicle contents and environment. Contextual targeting is used to match an ad about a university admission for someone watching a YouTube learning course, and an ad on a new makeup mirror might be displayed for those watching a make-up artist video. On the other hand, behavioural targeting, also known as a retargeting technique, is used to track and personalise user ad content based on their digital footprints from web visitation, app usage, physical locations, and search keywords (Bozdag, 2013). In this case, a user might be algorithmically tagged as interested in a UV skin protection cream if his/her location is tracked around a beach. Neither contextual nor retargeting is relevant without the algorithmic access and usage of cyber data.

This has been a worldwide-industrial phenomenon to the extent that, if the global advertising spending for the year 2021 is bifurcated into traditional and algorithmic bases, traditional ad spending on TV and broadcast radio only receives 13% of the global ad spending (Statista, 2021). Subsequently, experts and practitioners have contested that several benefits, including customisation, personalisation, contextualisation, cost reduction, accountability, evaluation, measurements, and many more are responsible for the accelerated prevalence of algorithmic advertising (Goldfarb, 2014). However, none of these benefits could have come to be to the algorithmic targeting and profiling models. In algorithmic targeting, every tidbit of digital users' activity and footprint is either a deterministic or probabilistic data point, both of which are at the core of every personalised ad campaign's effectiveness, viewability, and accountability (Kant 2021).

Even though both the supply and demand sides of the transactional models of algorithmic targeting are unanimous on the economic and the moral justifications of the commercialisation of personal data. As for the data suppliers like Google and Facebook, the data-for-free-services model underpins the economic benefit of algorithmic profiling (Chan-Olmsted, 2019).

Personalised advertising invites numerous legal issues of sensitivity, prohibited content, unfair commercial practices, data controlled liability, and content manipulation such as deep fake. Legal matters of personalised advertising have recently been debate due to the process argued to be built on customers' data vulnerabilities may highly influence their decision-making in concluding the transaction, thus impairing the lawful process of personal data collection.

The process which is based on algorithmic targeting created a major challenge as online users inadvertently surrender their data, routines, behaviour, patterns, interests, and preferences through tracking and surveillance (Basarudin, 2022). As such, algorithmic tracking invades human informational privacy as no one consents to constant surveillance, and reasonable people would expect their activities online or offline would be private. Meanwhile, experts have bemoaned the level of legal regulations on access, mining, and usage of cyber personal data (Eslami et al., 2018). Accordingly, it appears that advertisers have no limit to what type of information can be algorithmically tracked, stored, and used for algorithmically profiling audience, and in turn, cyber users are subjected to hyper-personalisation to the point of irritating or causing some level of psychological stress, manipulation and privacy breaching on targetted users (Campbell et al. 2020; Kietzmann et al. 2020). Therefore, this analysis will attempt to resolve the debate on how the existing laws adequately address cyber users' privacy and security against the misuse and abuse of personal data in personalised advertising.

3.0 Methods

This study adopts doctrinal legal methods by analysing the primary and secondary data. Primary data consists of statutory provisions, cases, legal rules, and principles of international instruments. The doctrinal legal method involves composing a descriptive, analytical, critical and detailed analysis of the existing authoritative legal materials, particularly Malaysia PDPA 2010, to allow the researcher to review and make recommendations to amend, repeal and replace the existing law to address the issues. Legal analysis is conducted concerning the European Union General Data Protection Regulation (GDPR) through a referral method, whereby the suggestions are based on their suitability to local circumstances. The provisions of the GDPR are significant to be referred to due to their relevancy, advance, and comprehensiveness in tackling the issues of personal data manipulation in the algorithmic profiling process.

4.0 Discussion on the legal analysis of personalised advertising

Malaysia PDPA 2010 has been an avenue to provide solutions for personal data protection issues. There are provisions specifically discussed on the requirement to comply with the principles listed under the Act which most of the principles are in *pari materia* and consistent with the GDPR such as regarding the processing of sensitive and lawful purposes, issue of consent and others. Moreover, the issue involves the monitoring and tracking of the behaviour of data subjects profiling and prediction is fall under the purview of the GDPR, thus making the online tracking activity within the local jurisdiction subject to the EU GDPR. The following sections present the silent theme of the principles and standards discussed in the GDPR to be observed by the data processor to ensure the lawful processes and protection of misuse of personal data.

4.1 Reasonable expectation of privacy test

Article 8 of the European Convention of Human Rights (ECHR) is one of the fundamental rules of the protection of rights of one's private life, such as lifestyle, sexual orientation, medical records, and so forth. Given that algorithms' access to personal data knows no limit as all types of data, including those that are not publicly accessible, are mined by algorithms, this rule provides a solid insight to data suppliers, aggregators, and processors to limit the mining and usage of publicly available data. The sensitivity of tracking and using personal data for targeting can extend far and beyond. Everyone expects their private life to remain private. For instance, when a user is algorithmically tagged as being interested in sexual behaviour or a sexual product that the user is not willing to publicise, the outcome of such profiling might be threatening to the user. However, the rule of expectation of privacy depends on several factors, including location, nature of the objects, and nature of the data itself.

The Court*, in the case of *P.G and J.H. v The United Kingdom,* states, "the concept of private life was broad, and there are several elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are recorded or reported in a public manner, a person's reasonable expectations of privacy may be a significant, although not necessarily conclusive factor."

The rule of reasonable expectation of privacy is inapplicable in public spaces where all the conversation can be heard. Indirectly, ones could not expect their information and communication online to be protected. However, privacy is not about the absence of information about oneself in the mind or knowledge of others, rather, it suggests control over information about a person. More so, algorithms might be smart enough to capture more than the needed information and details to profile users, it behoves the reasonable human who put the algorithms to used to ensure balance and reasonably decide when and to what extent their information should be communicated to others.

5.0 Findings under the General Data Protection Regulation

GDPR applies to data processors and controllers to adhere to the method of processing personal data to comply with the principles and legal obligations (De Hert & Czerniawski, 2016). The data processor is the legal person or other body which processes personal data subject while the controller is a person or the body that determines the purposes and means of the processing. In this context, the data processor includes Facebook, Google, Apple app so on and so forth.

The significant connotation of 'personal data' under GDPR refers to information related to a person's private life *stricto sensu* (in the strict sense), including any information related to an identified or identifiable living individual. Different pieces of information, which are collected together, can lead to the identification of a particular person, also constitute personal data. It refers most especially to the information on an individual's activity and routine, such as financial data or social behaviour. The definition is widely interpreted under GDPR to cover information about an individual's movement, preference, behaviour, and characteristics. From all indications and considering the rate at which online purchasing is globally preferred, there could be no doubt that algorithms are mining information to profile and segment users within the product universe. For one, previous researchers have bemoaned the possibilities of algorithm discrimination. However, in addition to that, users may become susceptible to various cyber and physical attacks or theft if people's financial information is not well managed. More so, access to financial information can also breed extreme consumerism, which can severely affect physiological and social well-being. Moreover, algorithmically mining personal information, including an individual's purchase behaviour, routine, and preference, might fall under hyper-personalisation according to personal data protection principles stipulated in the GDPR (Sakamoto & Matsunaga, 2019).

The GDPR imposes data protection principles about the automated processing of personal data, stated in Article 4(4), known as 'data profiling,' to ensure its proportionate usage and individual rights are observed. Therefore, advertisers and data aggregators must tread with caution and ensure a between personalisation and hyper-personalisation, especially regarding information related to financial behaviour, status, and habits (Batista et al., 2020).

5.1 Data Protection Principles

Article 5(1)(a) of the GDPR requires the process of data profiling to be lawful, fair and transparent to ensure data quality. Data profiling should not only have a lawful basis but also comply with Article 9 regarding the processing of special categories of personal data. Article 9 listed several categories of personal data which is prohibited from being processed, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data to identify a natural person's sex life or sexual orientation. However, the concept of fairness and transparency is questionable as the profiling process in personalised advertising is often invisible to the data subject (Lee, 2020). The process may collect more personal data than they need and includes types of data which are prohibited to be processed. Therefore, in complying with Article 5(1)(a) on lawful and fairness and 5(1)(c) on the principle of data minimisation, personalised advertising the data collector and data processor should include connotations and provisions informing the data subjects of the need to collect personal data, how it is collected and how it should be used.

5.2 Lawful Bases for Processing

Simultaneously, personalised advertising data processors must observe the concept of consent as a basis for lawful profiling processes (De & Imine, 2020). Consent of the data subject stated in Article 4(11) of the GDPR is valid if it is freely given, specific, informed and unambiguous. The consent must be 'informed' to uphold the transparency principle. The purpose and how data profiling is being conducted should reach the knowledge of the data users to obtain unequivocal, understandable and accessible consent otherwise, the consent will be considered invalid. Moreover, personal data profiling, which is based on derived and inferred data from other sources rather than directly from the data subjects, must be understood to represent an informed choice (Pawlata & Cakir 2020). Besides, the consent given must also be easily withdrawn to effectively show that such terms are accessible. This could be represented by the act of selecting yes or no to express an agreement on the internet website such as cookies or any other statement or conduct which signifies acceptance and consent to the processing of personal data.

* 25 September 2001, European Convention on Human Rights Judgement.

5.3 Special categories of data

Personalised advertising, which is based on data profiling, may fall under the exception of a special category of data prohibited from being processed if it meets conditions under Article 9(2) of the GDPR; among it, if the data subject has given explicit consent to the processing of those personal data. For example, if profiling may infer someone's state of health from the quality or special ingredient of a food shopping record, consent must be obtained by the data subject.

6.0 Conclusion and Recommendations

The EU GDPR has long been referred to as it provides an avenue to protect the processing of personal data. Individuals' data, either directly or indirectly available online, is considered their private information. Thus, profiling people's data for tracking and targeting advertising must observe certain criteria mainly on the issue of consent and minimisation data. Therefore, the controller should deliver clear and concise information to the data subject regarding the category of data that will be used in profiling, what is the impact of data profiling so on and forth. Besides, the data subject must be given options either to accept or reject tracking to consider consent is freely given.

On the other hand, the protection and safety of individuals' personal data rely on the controller and processor. The algorithms system should be based on security by-designed whereby the system development is actually performing as intended and complied with the agreed standard. Further studies should incorporate the response of the consumers on personalised advertising to ensure the law is able to protect their privacy.

7.0 Limitation

The activities of personalised advertising or tracking-based advertising have been exercised by the data processor and controller over the internet. The law which is regional in nature makes the enforcement of privacy and personal data protection law beyond geography borders to be the limitation and constraint in this study. Therefore, the provisions and practical guidelines for the lawfulness process of personalised advertising should always be reviewed to address the issue.

Acknowledgements

This paper has received no specific grant from any funding agency in the public, commercial, or non-profit sectors.

Paper Contribution to Related Field of Study

This study offers instructive insights into the context of personalised advertising and algorithmic targeting. Specifically, this paper deduces some important implications of personalisation and algorithmic targeting on online data protection from the EU GDPR. By so doing, this study acknowledges the value of algorithmic targeting in personalised advertising as well as the value of personal data, but also highlights the importance of data protection against misuse, abuse, and hyper-personalisation. The doctrinal analysis presented in this study underscores the benefit of algorithmic targeting to cyber users, data aggregators, and advertisers. Moreover, without statutory regulation and standards, cyber personal data protection might be jeopardised. Subsequently, this study exemplifies some of the implications of personalized advertsising on data protection and the law to address the issue.

References

Barbu, O. (2014). Advertising, microtargeting and social media. *Procedia-Social and Behavioral Sciences*, 163, 44-49.

Basarudin, N. A., Yeon, A. L., & Yusoff, Z. M. (2022). The role of cybersecurity law for sustainability of innovative smart homes (Goal 9). In *Good Governance and the Sustainable Development Goals in Southeast Asia* (pp. 110-117). Routledge.

Batista, M., Fernandes, A., Ribeiro, L. P., Alturas, B., & Costa, C. P. (2020, June). Tensions between privacy and targeted advertising: Is the general data protection regulation being violated?. In *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-5). IEEE.

Blass, J. (2019). Algorithmic advertising discrimination. *Nw. UL Rev.*, *114*, 415.

Bozdag, E. (2013). Bias in algorithmic filtering and personalization. *Ethics and information technology*, *15*(3), 209-227.

Cabañas, J. G., Cuevas, Á., & Cuevas, R. (2018). Unveiling and quantifying facebook exploitation of sensitive personal data for advertising purposes. In *27th USENIX Security Symposium (USENIX Security 18)* (pp. 479-495).

Campbell, C., Sands, S., Ferraro, C., Tsao, H. Y. J., & Mavrommatis, A. (2020). From data to action: How marketers can leverage AI. *Business Horizons*, *63*(2), 227-243.

Chan-Olmsted, S. M. (2019). A review of artificial intelligence adoptions in the media industry. *International Journal on Media Management*, *21*(3-4), 193-215.

De Hert, P., & Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law*, *6*(3), 230-243.

De, S. J., & Imine, A. (2020). Consent for targeted advertising: the case of Facebook. *AI & SOCIETY*, *35*(4), 1055-1064.

Eslami, M., Krishna Kumaran, S. R., Sandvig, C., & Karahalios, K. (2018, April). Communicating algorithmic process in online behavioral advertising. In *Proceedings of the 2018 CHI conference on human factors in computing systems* (pp. 1-13).

Faggella, D. (2018). AI in the life sciences: six applications. *Genetic Engineering & Biotechnology News*, *38*(9), 10-11.

Goldfarb, A. (2014). What is different about online advertising?. *Review of Industrial Organization*, *44*(2), 115-129.

Hazelwood, K., Bird, S., Brooks, D., Chintala, S., Diril, U., Dzhulgakov, D., ... & Wang, X. (2018, February). Applied machine learning at facebook: A datacenter infrastructure perspective. In *2018 IEEE International Symposium on High Performance Computer Architecture (HPCA)* (pp. 620-629). IEEE.

Kant, T. (2021). Identity, Advertising, and Algorithmic Targeting: Or How (Not) to Target Your "Ideal User".

Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat?. Business Horizons, 63(2), 135-146.

Lee, S. (2020). A Study on Consent of the GDPR in Advertising Technology focusing on Programmatic Buying. *Available at SSRN 3616651*.

Lenca, M., & Andorno, R. (2017). Towards new human rights in the age of neuroscience and neurotechnology. *Life sciences, society and policy*, *13*(1), 1-27.

Noel, J. K., Babor, T. F., & Robaina, K. (2017). Industry self-regulation of alcohol marketing: a systematic review of content and exposure research. *Addiction*, *112*, 28-50.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Pawlata, H. and Cakir, G. (2020) *The impact of the transparency consent framework on current programmatic advertising practices.* In: 4th International Conference on Computer-Human Interaction Research and Applications - Volume 1

Sakamoto, T., & Matsunaga, M. (2019, May). After GDPR, still tracking or not? Understanding opt-out states for online behavioral advertising. In *2019 IEEE Security and Privacy Workshops (SPW)* (pp. 92-99). IEEE.

Statista (2021). Growth of advertising spending worldwide in 2021, by medium. Available at: https://www.statista.com/statistics/240679/global-advertising-spending-growth-by-medium/

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019. Profile books.