

Legal Analysis of The Privacy Paradox between Consumer Convenience and Personal Life Intrusions in Hyper-Personalised Advertising

Noor Ashikin Basarudin^{1*}, Roslizawati Ahmad², Ridwan Adetunji Raji³,
Nur Fatin Nabila Abd Rahman⁴

* Corresponding Author

¹ Faculty of Law, Universiti Teknologi MARA Pulau Pinang, Permatang Pauh Campus, 13500 Pulau Pinang, Malaysia, ² Faculty of Business and Management, Universiti Teknologi MARA Pulau Pinang, Permatang Pauh Campus, 13500 Pulau Pinang, Malaysia,, ³ College of Communication and Media Sciences, Zayed University, Abu Dhabi, United Arab Emirates, ⁴ Academy of Language Studies, Universiti Teknologi MARA Pulau Pinang, Permatang Pauh Campus, 13500 Pulau Pinang, Malaysia

noorshikin@uitm.edu.my, roslizawati@uitm.edu.my, ridwan.raji@zu.ac.ae, nurfatin3364@uitm.edu.my
Tel: +60133568206

Abstract

This paper examines the privacy paradox in hyper-personalised advertising, where consumers enjoy increased convenience while unknowingly exposing themselves to deeper personal data intrusions. Driven by extensive algorithmic profiling, hyper-personalisation raises concerns of covert surveillance, behavioural manipulation, and diminished autonomy. Using a doctrinal legal method, the study analyses the Malaysian Personal Data Protection Act 2010 in comparison with the EU GDPR. The findings reveal significant regulatory gaps in transparency, consent validity, and accountability for profiling practices. The paper concludes that stronger legal safeguards and clearer ethical obligations for data controllers are essential to balance consumer convenience with meaningful privacy protection.

Keywords: Hyper-Personalised Advertising; Algorithmic Targeting; Personal Data Profiling; Data Protection

eISSN 2514-7528 © 2026. The Authors. Published for AMER by e-International Publishing House, Ltd., U.K. This is an open access publication 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).

DOI: <https://doi.org/10.21834/jabs.v11i32.487>

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 early online advertising targeting techniques. Hyper-personalisation in digital advertising refers to the process of collecting much of information on the needs, preferences, and interests of the existing and potential clients through a complex and distinctive approaches (Singh & Kakkar, 2025), such as psychographic segmentation, cross-site tracking, social media analytics, geofencing, IP matching, and practices that 'listen' to what consumers say, listen to, or watch to enable business to provide customers with precisely what they desire (Parshetty et al., 2024) as illustrated in figure 1.

Individual personal data are easily accessible online as we exchange data while browsing websites, communicating via social media, and searching for information on search engines (Limba & Šidlauskas, 2018; Alhabash et al., 2017). Algorithms act as an enabler for advertisers to utilise this data to personalize ads, target specific persons, increase the engagement, and adjust price and costs of services and goods (Beauvisage et al., 2024; Alavi et al., 2024).

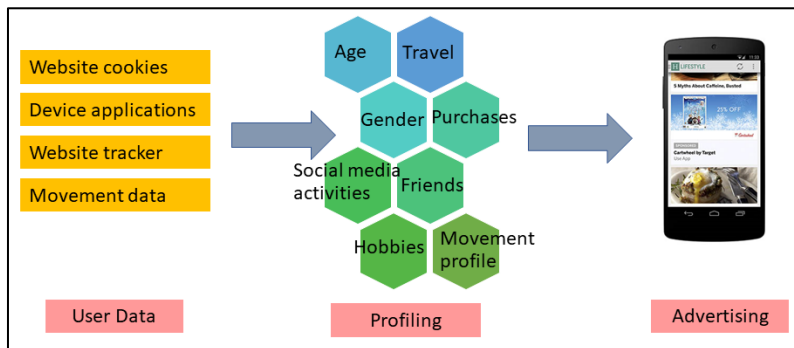


Figure 1: User Profile Construction for Hyper-Personalised Advertising
(Source: Author's Illustration)

Hyper-personalisation enhances customer engagement and effectively reaching specific target audiences by generating and delivering original and distinctive content to encourage relevant and relatable communications, providing excellent and create more compelling customer experiences to make purchase, fostering loyalty and retention, and driving sales growth (Gallery, 2024; Singh & Kakkar, 2025). To a certain extent, an impactful hyper-personalisation enables prediction of future trends allows for the development of more effective marketing and advertising tactics (Pandey, 2025).

However, in this regard, it brings to a distortions and disruptions of "privacy paradox" in hyper-personalized advertising where the conflict between consumers' perceived

benefits of convenience and tailored experiences and their concern about the potential invasion of privacy through data collection (Yaghmourian, 2024; Buck et al., 2014; Kehr et al., 2015; Zafeiropoulou et al., 2013; Zhang et al., 2014). Legally, this paradox involves the need for businesses to balance the right to freedom of expression with the right to privacy, particularly regarding data collection and use in advertising (Maria, 2025). For example, businesses entity might argue that targeting ads is part of their free expression and innovation while the tracking and profiling of consumer information without full understanding or control violates their privacy (Kim, 2024; Davenport et al., 2020).

On the contrary, the evolving nature of this technology constantly challenges the boundaries of privacy. The privacy paradox runs mainly unconsciously, making it even more prone to lead to risks (Barth & De Jong, 2017). These are multifaceted and far-reaching, from privacy violations and data breaches to the manipulation and exploitation of user data by the companies. An increase in data correlates with an elevated risk of breaches, leaks, or abuse. Although data protection laws have been in effect for years, numerous businesses continue to implement data protection rules inadequately or inappropriately (Sirur et al., 2018; Ullagaddi, 2024).

Further, the ambiguity of the regulations, while beneficial in certain respects, undeniably serves as a conduit for exploitation and misconduct. Additionally, the concerns linked to hyper-personalization encompass not only possible privacy infringements but also the manipulation of customer choices through the utilisation of gathered data (Bol et al., 2018). Thus, this research analyses the legal aspect of privacy disconnection in hyper-personalisation and the Malaysia Personal Data Protection Act in comparative with European Union General Data Personal Regulation to address the issues.

2.0 Literature Review

Personalized communication is often used to deliver the message at the right time to the right person in a cost-efficient way (Kim and Huh 2017). It involves incorporating elements in a message that refer to each individual recipient and are based on the recipient's personal characteristics and information (Guo, & Jiang, 2025; Baek and Morimoto 2012; Bang et al., 2019; De Keyser, Dens, & De Pelsmacker, 2015; Maslowska, Smit, & Putte, 2016). This personal information is mostly collected online. Next to personalizing the content of the message, advertisers can also monitor people's online behaviour and use the collected information to show people individually targeted advertisements. This practice, commonly referred to as targeted advertising or online behavioural advertising (Boerman et al., 2017; Varnali, 2019), encompasses hyper-personalised advertising, in which personal information is collected and used to deliver online messages tailored to specific individuals either by adapting the content itself (content personalisation) or by selectively exposing particular users to the message (individual targeting) with the aim of ensuring customer inclusivity.

The level of personalization of an ad is based on the type of data that is used to target the ad, and the amount of information that is used (Kumar et al., 2025; Boerman,

Kruikemeier, and Zuiderveen Borgesius 2017). Advertisers can use a wide range of types of information, such as demographic data (e.g., name, age, gender), location, online shopping behavior, click-through responses to ads, and communication content (e.g., emails, social media posts; Aguirre et al., 2015; Boerman et al., 2017; Kim & Huh, 2017).

The nature and content of these types of information influence the perception of how private this information is perceived, and thus probably the extent to which people believe it is acceptable when advertisers collect and use this information. Research has shown that people's perceptions of personalized advertising and its effects vary depending on the type of data that is used to create the ad. Malheiros et al. (2012) found that people felt less comfortable when an ad was showing a person's photo, name, or age, compared to when the ad mentioned the holiday destination they were searching for. Furthermore, research has shown that adding personal information (e.g., name, age, transaction information, and/or location) to a targeted ad (based on browsing history) makes it more intrusive (Van Doorn and Hoekstra 2013) and make people feel more vulnerable (Aguirre et al., 2015).

However, different people may respond to the practice differently as may be explained by the notion that people do not consider all personal information as equally personal or privacy sensitive (Salih et al., 2025; Walrave, et al., 2018). There are two reasons why people perceive some types of information to be less acceptable than others. First, types of information used to personalize and target advertising can be categorized as individual-specific that can identify an individual without additional information (i.e., name, identification number, or facial recognition data), or information that is not individual-specific that can only identify or trace back to you when it is combined with additional information (i.e., online behaviour, location, purchases).

In the context of personalized advertising, people have a stronger feeling of psychological ownership regarding individual-specific information because they can be directly identified by such information, and thus is truly 'their information' (Jussila et al., 2015; Pierce, Kostova, and Dirks 2003). As not individual-specific information does not directly identify a person and could also apply to many others, this type of information will cause less feelings of ownership. Therefore, we expect that people will have a greater tendency to protect individual-specific information, and the perceptions of the use of individual-specific information to personalize advertising are likely to be more negative compared to not individual-specific information (Pierce et al., 2003).

Although people do understand that companies collect and use personal information online (McDonald and Cranor 2010; Smit, Noort, & Voorveld, 2014), they may not accept the collection and usage of all types of information. Communication privacy management theory (Petronio 2012) and information boundary theory (Sutanto et al., 2013) propose that people create rules or boundaries regarding who is denied or granted access to specific personal information. When information is perceived to be too personal or when they expect information to remain private (i.e., personal communication), advertisers cross such a boundary or rule, which may disturb them making people feel anxious or uncomfortable (Sutanto et al., 2013).

The privacy paradox refers to the discrepancy between consumers stated preferences for privacy and their online behaviours. It has been thoroughly documented that consumers prefer to disclose less information than they actually do (Awad and Krishnan, 2006) and, so far, research has focused on behavioural factors that may explain this paradox (Barari et al., 2024; Hui et al., 2007; Li et al., 2017; Taddicken, 2014).

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 debated 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 (Salih, et al., 2025).

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).

3.0 Methodology

This study adopts doctrinal research methodology by systematically analysing legal principles, statutory provisions, case law, rules, principles and regulatory frameworks relating to hyper-personalised advertising and privacy. The doctrinal legal method encompasses a descriptive analysis, analytical, critical and detailed analysis of the existing authoritative legal materials, 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 to comparatively determine the scope, definitions, and legal protections offered in the intended jurisdiction including Malaysia and European Union. This research further synthesises and evaluates the interpretation of the legislative. The jurisdictions of the European Union legal framework General Data Protection Regulation (GDPR) are considered as EU laws are widely regarded as the most comprehensive and influential data protection law in the world. Thus, Malaysia, as an open digital economy, must align with such international standards and best practices.

4.0 Privacy Challenges in Algorithmic Hyper-Personalised Advertising Ecosystem

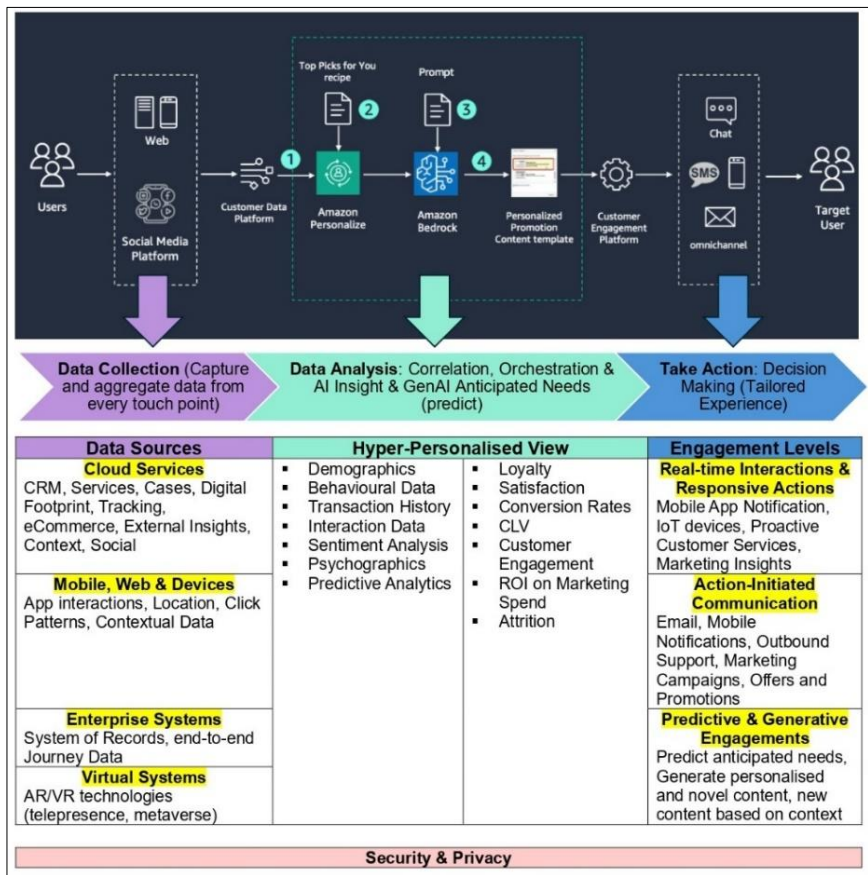


Figure 2: Hyper-Personalisation Decision Making Process
(Source: Author's Illustration)

Privacy presents significant challenges in the algorithmic advertising ecosystem, primarily because the effectiveness of such advertising heavily relies on the collection, analysis, and utilisation of vast amounts of Personal Identifiable Information (PII) including personal details, browsing habits, location data, and more. The process of hyper-personalisation is illustrated in Fig. 2 where PII of customers is collected through a variety of techniques and data sources. These methods are often designed to track and analyse user behaviour across online platforms to enable highly targeted advertising among it includes web and mobile tracking such as cookies, device fingerprint, and pixel tags. Besides, business might

collect the PII through customer registration or survey feedback form. Meanwhile, the plugins system in social media platform including Facebook, X, Instagram, and TikTok may allow websites integration such as “Like” and follow buttons (Femi-Adeyinka et al., 2024), social counter displays, and “repost” that allow the social media platform to track the user’s browsing behaviour even when they are not logged into their social media account (Salih, et al., 2025; Kubovics & Zaušková, 2020; Perakakis et al., 2019).

The collection stage of user data in Fig. 2 is basically through cloud services including digital footprint and tracking, history of movement data, website cookies, usage of device applications and website tracker, business customers’ records as well as virtual record of good purchase such demonstrated in import dataset Amazon.

The next process involves the stage of training model using top identifying and targeting specific customer segments. The information will be segmented and profiled according to the interest of a group of people through the algorithmic process of predictive analytics and import prompt with personalise recommendation into online business system bedrock such as Amazon. Finally specific online users will be fed with advertisements related to their interests and needs at the engagement level based on recommendations and prompt through real-time interaction, action-initiated communication and predictive engagement.

Data processing can have various implications for data subjects in different social contexts that are covered by their fundamental rights. For example, a person’s privacy is affected in its classic function to exclude other people from her private sphere if the processing of data leads to a disclosure of her private information that she actually wanted to shield from other people. By linking such data processing to a data protection law takes into account the data subject’s need to be able to decide whether or not to go public and what information to disclose about herself. User profiling and targeted advertising potentially expose sensitive and damaging information about consumers including privacy violations, data manipulation and its influence on consumer decisions, and discriminatory potential.

4.1 Privacy Violations

Users who frequently disclose detailed personal information such as location, interests, and life events heighten their vulnerability to privacy breaches by generating more data points that third parties can exploit. A major contributor to this risk is the granularity of privacy settings and the way users engage with them. Although digital platforms typically provide complex privacy controls, many individuals fail to configure these settings or misunderstand their implications (Zehnle, et al., 2025). Default settings are often overly permissive, enabling wider access to personal information than users intend. Failure to routinely review or adjust these settings, combined with granting third-party applications broad permissions, amplifies exposure to privacy harms. Hyper-personalisation systems intensify these risks through the extensive collection and processing of user data. They rely on two forms of information including explicit empirical data, voluntarily provided by users (e.g., name, email, personal details), and inferential data, generated by algorithms that deduce demographic traits or behavioural preferences such as age, gender, or political inclination.

These datasets feed into a continually evolving user profile that categorises individuals based on predicted tastes and interests (Salih, et al., 2025; Barari et al., 2024)

This profiling process creates profound autonomy risks. First, the user profile curation is performed by the personalization algorithm. This process is opaque to the user where inferences about their identity are being made without their conscious contribution towards the process. Second, this profile curation process is a dynamic process. Whenever the user interacts with the personalization algorithm, the algorithm captures data from that interaction and uses that knowledge to update the user profile (Rachmad, 2025). Personalized Digital Influence Theory. United Nations Economic and Social Council. In this sense, it must be understood that the system is not trying to predict an established static identity of the user. Instead, it is actively contributing to the identity formation process of the user by recursively updating its impressions about the user based on how the user reacts to choices that the personalization algorithm suggests (Kohli, et al., 2025).

Additionally, when the personalization algorithm categorizes a user, it does based on attributes that the algorithm determines are most relevant to the user and itself. For example, on an e-commerce website, the algorithm may categorize one of the user's interests "women's shoes" based on an instance of sale. This categorization could suffer from an accuracy problem if the user does not self-identify as being interested in "women's shoes." However, such a decision may inevitably be helpful to the system to more effectively show targeted ads about shoes. Here, the user's autonomy is getting impinged by being lumped into an erroneous category without their consent or knowledge. One might propose to correct inaccurate profiling by providing access to the user in a mutually collaborative process to fix errors. However, user identity on internet platforms and the user's perceived identity of themselves could significantly differ from the expectations of the system. For instance, research has shown that anonymity on the internet enables individuals to reveal more information than in real life, called the online disinhibition effect. This disinhibition also prompts users to overshare and sometimes conflate the truth, further exacerbating the inaccurate identity profiling phenomenon (Saura, 2024; Barari et al., 2024).

4.2 Data Manipulation and Its Influence on Consumer Decisions

The concept of nudging can be understood as a behavioural economics equivalent to personalization technology as a mechanism to exploit existing human cognitive biases for customer's benefit. They propose a system called choice architecture which governs the way choices are presented to humans prompting them to take certain actions (Guo & Jiang, 2025; Al-Hadrawi & Jawad, 2024).

In other words, by designing how choices appear to an individual, one can prompt that individual to take certain actions. One example presented is how placing healthy foods in a school cafeteria at eye level while putting less-healthy junk food in harder-to-reach places causes individuals to opt more frequently to eat healthy foods. Wellness enhancing technology wearables exploit similar choice architecture systems to prompt users to take action towards their health.

This type of architecture design is called libertarian paternalism. It is paternalistic in that it guides you to make choices that will leave you better off. It is libertarian in that the extent of influence the architecture has over been merely guidance. An individual is free to opt-out. The possibility to opt out is said to "preserve freedom of choice." When a designed choice no longer serves the user's best interests, it shifts from a permissible nudge to a form of covert manipulation. Dark patterns in user interfaces exemplify this shift, as they intentionally exploit user behaviour and introduce significant risks of hidden manipulation (Krcan, & Urbanik, 2024).

Dark Patterns in user interfaces are a perfect example of how choice architecture is exploited to advance business interests removing interface design from the realm of nudge to the realm of covert manipulation. Dark patterns are features of user interface design that are placed with the intention to trick users to perform actions they have not resolved to perform. Dark patterns either make it intentionally difficult for a user to perform an action that may hurt a website's business (account deletion) or prompt users to take actions that a user does not intend to take to help a website's business (auto-renewal subscriptions) (Guo & Jiang, 2025; Al-Hadrawi & Jawad, 2024).

The term "roach motel" refers to a dark pattern which the user finds very easy to get into but very difficult to get out of. For example, when a user attempts to cancel commercial website subscription, it takes the user a series of landing pages with various inputs and scrolling mechanisms before finally providing a 'cancel' option (Sheil et al., 2024).

"Forced continuity" is another type of dark pattern where user subscriptions are automatically renewed by making it extremely unintuitive to cancel subscription services. Dark patterns are inherently manipulative because they exploit interface design to deliberately steer users toward particular actions. Within the lens of normative autonomy rights, such practices undermine an individual's ability to act on reasons and decisions formed through their own autonomous judgment. This threat to personal autonomy becomes especially pronounced when dark patterns are engineered to create user dependency on digital services for the purpose of maximising engagement (Kumar et al., 2025).

5.0 Court Decision of other Jurisdictions

In the *Bundeskartellamt v Meta Platforms (2023)*, Bundeskartellamt's (German Federal Cartel Office) 2019 found that Meta Platforms, Inc. (formerly Facebook) abused its dominant position in the German market for social networking services. Meta was accused of collecting and combining user data from Facebook, Instagram, WhatsApp, and third-party websites through embedded tools. The data combination enabled precise ad targeting, giving Meta a commercial advantage in digital advertising. The Bundeskartellamt found that, users were forced to accept data merging as a condition for using Facebook services. It ruled that Meta's practice violated the GDPR, particularly Articles 6 and 9, concerning lawful basis and sensitive data. The authority concluded that the unlawful data processing also strengthened Meta's market dominance, amounting to abuse under

Section 19 German Competition Act 2021. Meta appealed, arguing that data protection law and competition law are separate domains. Meta claimed users gave valid consent and that data processing was necessary for contract performance.

The European Court of Justice (ECJ) confirmed that competition authorities may consider GDPR compliance when evaluating abuse of dominance. However, they must cooperate with data protection authorities under the principle of sincere cooperation Art. 4(3) Treaty on European Union (TEU). The Court held that dominance can undermine free consent, making bundled consent invalid. It ruled that personalized advertising is not necessary for fulfilling a social media contract under Article 6(1)(b) GDPR. Meta's reliance on legitimate interest also failed, as users' privacy rights outweigh commercial interests. The ECJ clarified that even inferred sensitive data triggers Article 9 GDPR protections. The judgment linked data volume and privacy to competition parameters, recognizing data as a source of market power. It affirmed that GDPR breaches can signal abusive conduct by dominant firms. Meta was thus found to have exploited users' lack of choice and distorted competition through unlawful data practices.

In other words, Meta's data practices especially bundling and reliance on illegitimate legal bases as it violated users' autonomy and privacy rights. The ruling ultimately established that unlawful data extraction by a dominant platform can amount to exploitative conduct that distorts competition.

In the case of *Lloyd v Google LLC (2021)*, Richard Lloyd brought a representative action on behalf of approximately 4 million iPhone users, claiming that Google had unlawfully processed their personal data in breach of the United Kingdom Data Protection Act 1998 (DPA 1998). The case arose from Google's use of "Safari Workaround" technology, which allegedly allowed it to track users' internet activity without consent while they used Apple devices. Lloyd argued that users' personal data had been processed without proper consent and sought compensation on behalf of the class for the "loss of control" over their personal information. He relied on the representative action mechanism under Civil Procedure Rules (CPR) 19.6, asserting that all class members shared the "same interest" in pursuing damages.

The UK Supreme Court unanimously dismissed Lloyd's claim and ruled in favour of Google. The Court held that under section 13(1) of the DPA 1998, compensation requires proof of either material damage (such as financial loss) or distress caused by the unlawful processing. Mere "loss of control" over personal data, without evidence of actual harm, does not constitute compensable damage. Consequently, the claim could not succeed on the basis of abstract privacy infringement alone.

The Court also addressed the representative action framework, clarifying that while the "same interest" test under CPR 19.6 is satisfied when the representative and class members have aligned legal interests, the court retains discretion to refuse permission if the action is unworkable or requires extensive individualised proof. In this case, damages would have depended on showing individual harm for millions of users, making collective proceedings impractical.

Although the UK Supreme Court ultimately ruled that “loss of control” alone did not constitute compensable harm under the DPA 1998, the judgment underscores a broader principle: companies must respect individuals’ rights to control their personal data. To reconcile convenience with privacy, Google and other data controllers are obligated to obtain valid, informed consent, ensure transparency, and provide meaningful choice, thereby upholding the normative rights of users while still delivering personalised services.

6.0 Malaysia Legal Approach on Hyper-Personalised Advertising

In Malaysia, the regulatory landscape governing hyper-personalised advertising is shaped by the Consumer Protection Act 1999 (CPA 1999) that prohibits misleading, unfair, or aggressive advertising practices. Meanwhile, the Communications and Multimedia Act 1998 (CMA 1998) impose content-based obligations to ensure that digital advertisements do not contain false, indecent, or harmful material, and the Personal Data Protection Act 2010 (PDPA 2010) controls the lawful collection and use of personal data for targeted marketing

Section 3(1) of CPA 1999 of Malaysia defines ‘advertisement’ as every form of advertisement, whether or not accompanied by or in association with spoken or written words or other writing or sounds and whether or not contained or issued in a publication, and includes advertisement: a) by the display of notices; b) by means of catalogues, price lists, circulars, labels, cards or other documents or materials; c) by the exhibition of films or of pictures or photographs; or d) by means of radio, television, telecommunication or any other similar means.

Although there are no specific provisions that explicitly mention or exclusively regulate personalised advertising, but the CPA 1999 can still apply when hyper-personalised ads contain elements that fall within prohibited commercial conduct. In particular, personalised advertising may breach the CPA when the content or targeting method amounts to misleading or deceptive advertising as discussed in Section 9 for instances if the advertisement creates false impression tailored to an individual user, exaggerates benefits based on behavioural profiling, hides material information predicted to be “irrelevant” to that user, or presents dynamic pricing that misleads one consumer compared to others.

All content that is advertised online must adhere to the CMA 1998 and the Malaysian Communications and Multimedia Content Code (CMCC). Under Section 211 of the CMA 1998, any content that is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person is prohibited. This section is applicable to hyper-personalised advertising where AI-driven targeting delivers false, manipulated, or fabricated content, such as tailored claims, manipulated reviews, or untrue “limited stock just for you” prompts because the provision prohibits the transmission of any false or misleading information through digital networks, and personalised delivery to a single profiled user still constitutes content provided within the meaning of the Act.

Hyper-personalised advertising enables unprecedented data collection, aggregation, and repurposing often without users’ knowledge or meaningful recourse. This creates an asymmetry of informational power, allowing data controllers to influence individuals’

autonomy in consuming goods and services. Accordingly, this imbalance underscores the urgent need for robust personal data protection laws that impose stricter transparency, consent, and accountability obligations on data controllers to safeguard users' informational autonomy.

7.0 Due Process of Data Handling in Hyper-Personalised Advertising

Malaysia's PDPA 2010 provides a foundational framework for regulating the collection and processing of personal data, yet its protections remain more limited compared to the comprehensive and rights-based approach of the GDPR. Unlike the GDPR which imposes stringent obligations, extraterritorial reach, and enforceable data subject rights, the PDPA adopts a more sector-specific, consent-driven model that offers narrower safeguards against intrusive data practices such as hyper-personalised advertising.

7.1 Personal Data

'Personal data' is defined under Section 4 of PDPA 2010 as any information in respect of commercial transactions that is being processed automatically, recorded to be processed or recorded as part of a relevant filing system that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data controller. It includes any sensitive personal data or expression of opinion about the data subject.

Meanwhile, the concept of "personal data" within article 4(1) of the GDPR covered not only data collected and stored by a controller, but also included all information resulting from the processing of personal data relating to an identified or identifiable person, a string composed of a combination of letters and characters containing the preferences of a user of the internet or of an application.

Comparatively, Malaysia PDPA applies in narrow sense as only covers the processing of data in commercial transactions. Furthermore, Personal data also means information that to a data subject, but does not explicitly include IP addresses, cookies, location data, genetic data, etc. unless such data can clearly identify a person in context. Thus, in the context of hyper-personalised advertising, GDPR has broadly and inclusively protect the data subject as it expressly recognised almost all tracking and profiling activities used for hyper-personalisation especially algorithmic profiling shall automatically fall under strict data protection rules, including consent, transparency, and purpose limitation. Unlike, the PDPA 2010, many profiling technologies used in hyper-personalised ads may fall outside PDPA protection unless they clearly identify an individual, leaving room for weaker regulatory oversight.

7.2 Data Protection Principles

Article 5(1) of the GDPR establishes the core principles governing all personal data processing, setting out a framework based on: a) lawful, fair and transparent, b) purpose limitation, c) data minimisation, d) accuracy, e) storage limitation, f) confidentiality and

integrity, and g) accountability to ensure data quality and critically impose the accountability principle, which requires data controllers to demonstrate compliance.

In contrast, Section 5 of the Malaysian PDPA 2010 adopts a narrower approach by centring processing on the requirement of the data subject's consent and stipulating that organisations must comply with the PDPA's seven data protection principles. Unlike the GDPR's multi-basis model, where consent is only one of several lawful grounds for processing, the PDPA relies predominantly on consent, reflecting a more rigid legal structure. Furthermore, the GDPR's accountability principle imposes proactive obligations on data controllers, whereas the PDPA does not impose an explicit duty to evidence compliance unless an investigation arises.

Table 1: Data protection Principle under EU GDPR and PDPA 2010

Article 5 of EU GDPR	Section 5 of Malaysia PDPA 2010
Sets out seven key data protection principles:	Processing must comply with the seven PDPA Principles:
1. Lawfulness, fairness, transparency	1. General Principle
2. Purpose limitation	2. Notice and Choice Principle
3. Data minimisation	3. Disclosure Principle
4. Accuracy	4. Security Principle
5. Storage limitation	5. Retention Principle
6. Integrity and confidentiality (security)	6. Data Integrity Principle
7. Accountability	7. Access Principle

(Source: Author's Summary)

Data profiling should not only have a lawful basis but also comply with Article 9 GDPR 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.

In Schrems v Meta Platforms Ireland Ltd (formerly Facebook Ireland Ltd) [2025] 4 WLR 25, The data controller directed personalised advertising at the data subject, a user of the network domiciled in Austria, based on information it had received from outside sources concerning the data subject's sexual orientation and political views. The data subject, who not post any sensitive personal data on their Facebook profile, brought an action in an Austrian regional court seeking, inter alia, an injunction against the controller on the grounds that it had unlawfully processed, and stored for an indefinite period, their personal data contrary to Parliament and Council Regulation (EU) 2016/679 (the General Data Protection Regulation or "GDPR"). Subsequently, the data subject referred to their sexual orientation during a speech at a public panel discussion. The action and the data subject's appeal were dismissed. On the data subject's subsequent appeal, the Supreme Court, Austria, was of the opinion that the information concerning the data subject and processed by the controller, could be categorised as prohibited "sensitive" data within the meaning of

article 9(1) of the GDPR, but questioned whether the data subject had “manifestly made public” that data and, in so doing, had given his consent to the processing thereof under article 9(2)(e).

7.2.1 Fairness, Lawfulness, and Transparency

Table 1: Summary of data protection Principles under EU GDPR and Malaysia PDPA 2010.

Article 5 of EU GDPR		Section 5 of Malaysia PDPA 2010	
Principle of Lawfulness, Fairness, Transparency	• The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. • The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed.	Section 6: General Principle	• establishes consent as the principal basis for the lawful processing of personal data, subject to stricter controls for sensitive personal data • any processing, whether consent-based or exception-based, must pursue a lawful purpose directly connected to the data controller's functions, be necessary for that purpose, and involve data that is adequate yet not excessive.
		Section 7: Notice and Choice Principle	• data controller must inform subjects about data processing, purposes, sources, rights, third-party disclosures, choices, and consequences, ensuring transparency and accountability.
		Section 11: Data Integrity Principle	• data controller must ensure personal data is accurate, complete, not misleading, and up-to-date, considering its collection and processing purposes.

(Source: Author's Summary)

GDPR Article 5(1)(a) states that, “Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject”. This principle specifies that

organizations must ensure their practices around data collection don't compromise the law and that their use of data is transparent to data subjects.

Section 5 of the PDPA 2010 does not appear as a single combined principle, but the three elements reflected the GDPR principle of lawfulness, fairness and transparency. It includes the requirement of lawfulness aligns with the Section 6 the PDPA's General Principle, which mandates that personal data be processed for a lawful purpose and on the basis of the data subject's consent. The element of fairness is reflected both in the General Principle requiring that processing be reasonable and directly related to the intended purpose and Section 11 on Data Integrity Principle to ensure fairness by obligating organisations to maintain data that is accurate, complete, and not misleading.

Meanwhile, the GDPR's emphasis on transparency corresponds to the Section 7 PDPA's Notice and Choice Principle, which requires data users to clearly inform individuals about the purpose of processing, the types of data collected, and the choices available to them. Together, these PDPA principles collectively capture the substance of the GDPR's foundational requirement that personal data processing must be lawful, fair, and transparent.

However, the concept of fairness and transparency and the principles are questionable as the profiling process in hyper-personalised advertising is often invisible to the data subject. The process may collect more personal data than they need and includes types of data which are prohibited to be processed. In terms of lawfulness, hyper-personalisation often depends on extensive tracking and profiling through cookies, device identifiers and behavioural data, yet the consent obtained is frequently bundled, opaque or based on interfaces designed to nudge users into agreeing, undermining the PDPA's requirements of informed consent for lawful processing. Fairness is also compromised when advertisers use algorithmic profiling to infer sensitive characteristics or exploit behavioural biases, conflicting with the PDPA's Data Integrity Principle where processing must not be misleading or cause detriment to the data subject. Transparency is further eroded by the opaque nature of the adtech ecosystem, where users are not meaningfully informed about how their data is collected, analysed, categorised or shared, contrary to the Notice and Choice Principle's requirement that individuals be clearly notified of processing purposes and options.

To address these issues, the PDPA should be strengthened by introducing explicit provisions regulating profiling and automated decision-making, including a requirement for express, unbundled consent for behavioural tracking and hyper-personalised advertising. Enhanced transparency obligations should mandate clear disclosure of the types of data collected, the logic of profiling, and the third parties involved, while expanding the definition of personal data to expressly include online identifiers and inferential data. Incorporating an accountability principle akin to the GDPR would further require organisations to document, justify and assess the risks of hyper-personalisation, ensuring that the regulatory framework adequately responds to the intrusive and opaque nature of modern advertising technologies.

7.2.2 Purpose limitation & Data Minimization

Article 5(1)(b) and (c) of the GDPR on purpose limitation and data minimization respectively require personal data to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The purpose must be clearly defined, communicated to the data subject, and limited.

It is in parallel with the requirement under Section 6(2)(a) and (b) for personal data to be collected only for purposes directly related to the activity of the data user and must not be excessive in relation to that purpose.

In December 2021, the High Court in the case of *Genting Malaysia Berhad v Personal Data Protection Commissioner & Ors* [2021] MLJU 2847 held that the PDPA does not allow the Director-General of the Inland Revenue Board of Malaysia to make blanket demands for personal data in view of the protections afforded to data subjects under the PDPA. Such requests for data must be made in accordance with the law, and it should be ensured that the request satisfies the test of necessity, in that “the interference with the rights of data subjects must be proportionate to the reality as well as to the potential gravity of the public interests involved”, and “there must also be a specific instance as contemplated by the statute and not a general sweeping and inconsistent reasons for the disclosure to be given”.

Having linked it with the hyper-personalised advertising issue, definitely the practice violates as the hyper-personalised advertising often relies on extensive tracking including cookies, behavioural analytics, device fingerprints, inferred preferences without clearly specifying the purpose. Thus, to prevent the violation of the law and to allow technology advancement in advertising, the data controller must provide the data subject with clear and accessible information regarding:

- (a) the categories of data collected, including online identifiers and behavioural data;
- (b) the logic, parameters, or criteria used in profiling;
- (c) the purpose and consequences of such profiling on the data subject; and
- (d) any third parties to whom the personal data or profiling outputs may be disclosed.

8.0 Conclusion

The study reveals a persistent privacy paradox, where consumers benefit from enhanced convenience, relevance, and personalised digital experiences, yet simultaneously face unprecedented intrusions into their personal lives. The sophistication of behavioural tracking, algorithmic profiling, and inferential analytics enables advertisers to anticipate user needs with remarkable precision, but this same precision exposes individuals to opaque data practices, excessive surveillance, and loss of informational autonomy. Current legal frameworks particularly Malaysia's PDPA 2010 offer important baseline protections but remain insufficient to confront the evolving risks posed by modern hyper-personalisation. Gaps in purpose limitation, transparency, consent requirements, and profiling safeguards create regulatory blind spots that allow intrusive advertising technologies to thrive with minimal accountability.

A more robust and future-proof data protection regime must therefore recalibrate the balance between consumer convenience and personal privacy. Strengthening statutory provisions to expressly regulate profiling, define incompatible further processing, and require explicit opt-in consent for hyper-personalised advertising is essential to restoring user control. Enhanced transparency obligations and the expansion of personal data definitions to include online identifiers and inferential data would further ensure that individuals understand and can meaningfully manage how their data is used. Ultimately, addressing the privacy paradox demands not only legal reform but also a normative shift toward accountability, fairness, and respect for human dignity in digital ecosystems. Only through such an integrated approach can the benefits of personalisation be realised without compromising the fundamental rights of data subjects in an increasingly data-driven society.

Acknowledgement

The authors would like to acknowledge the support of the Universiti Teknologi MARA Cawangan Pulau Pinang, Malaysia and Zayed University, Abu Dhabi, UAE for providing their incredible support to produce this research.

Article Contribution to Related Field of Study

This article contributes to the broader field of privacy law, digital consumer protection, and technology-driven regulation by clarifying the legal implications of hyper-personalised advertising within a rapidly evolving digital economy. It advances scholarly understanding of the privacy paradox by demonstrating how consumers' pursuit of convenience simultaneously exposes them to non-transparent data practices and algorithmic influence. Through a comparative analysis of the Malaysia PDPA 2010 and GDPR, the study highlights key regulatory shortcomings and offers evidence-based recommendations for strengthening legal safeguards in Malaysia. Its findings support ongoing discourse on ethical data governance, responsible AI deployment, and the need for robust profiling accountability, thereby enriching cross-jurisdictional debates on digital rights and personal autonomy.

Authors Declaration

This article is an extended version of the original conference paper published in the E-BPJ, Vol 7 (22), Nov, 2022, 109-114.

References

Alavi, S., Iyer, P., & Bright, L. F. (2024). Advertisement avoidance and algorithmic media: The role of social media fatigue, algorithmic literacy and privacy concerns. *Journal of Digital & Social Media Marketing*, 12(3), 276-292.

Alhabash, S., Mundel, J., & Hussain, S. A. (2017). Social media advertising: Unraveling the mystery box. In *Digital advertising* (pp. 285-299). Routledge.

Al-Hadrawi, B. K., & Jawad, A. R. (2024). Cognitive marketing and strategic drift: an exploration of cognitive bias in marketing decision-making. *International Journal of Multidisciplinary Research and Growth Evaluation*, 5(1), 933-946.

Barari, M., Casper Ferm, L. E., Quach, S., Thaichon, P., & Ngo, L. (2024). The dark side of artificial intelligence in marketing: meta-analytics review. *Marketing Intelligence & Planning*, 42(7), 1234-1256.

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

Barth, S., & De Jong, M. D. (2017). The privacy paradox—Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review. *Telematics and informatics*, 34(7), 1038-1058.

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.

Beauvisage, T., Beuscart, J. S., Coavoux, S., & Mellet, K. (2024). How online advertising targets consumers: The uses of categories and algorithmic tools by audience planners. *New Media & Society*, 26(10), 6098-6119.

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

Bol, N., Dienlin, T., Kruikeimeier, S., Sax, M., Boerman, S. C., Strycharz, J., ... & De Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, 23(6), 370-388.

Bozdog, 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.

Davenport, T., Guha, A., Grewal, D., & Bressgott, T. (2020). How artificial intelligence will change the future of marketing. *Journal of the Academy of Marketing Science*, 48(1), 24-42.

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.
- Femi-Adeyinka, C., Kose, N. A., Akinsowon, T., & Varol, C. (2024, April). Digital forensics analysis of youtube, instagram, and tiktok on android devices: A comparative study. In *2024 12th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE.
- Gallery, C. (2024). Marketing to the hyper-connected consumer. In *Fashion Business and Digital Transformation* (pp. 143-177). Routledge.
- Goldfarb, A. (2014). What is different about online advertising?. *Review of Industrial Organization*, 44(2), 115-129.
- Guo, B., & Jiang, Z. B. (2025). Influence of personalised advertising copy on consumer engagement: a field experiment approach. *Electronic Commercial Research*, 25, 1281–1310.
- 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.
- Kim, H. Y. (2024). What's wrong with relying on targeted advertising? Targeting the business model of social media platforms. *Critical Review of International Social and Political Philosophy*, 1-21.
- Kohli, R., Gupta, S., & Gaur, M. S. (2025). Guarding Digital Privacy: Exploring User Profiling and Security Enhancements. *arXiv preprint arXiv:2504.07107*.
- Krpan, D., & Urbanik, M. (2024). From libertarian paternalism to liberalism: behavioural science and policy in an age of new technology. *Behavioural Public Policy*, 8(2), 300-326.
- Kubovics, M., & Zaušková, A. (2020, July). Possibilities of Display and Collection of Marketing Data From the Social Media. In *7th European Conference on Social Media ECSM 2020* (p. 144).
- Kumar, P., Dadwal, S. S., Modi, S., Ghouri, A. M., & Jahankhani, H. (2025). The Dark Side of Marketing. *Springer Books*.
- 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.
- Limba, T., & Šidlauskas, A. (2018). Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the Facebook. *Entrepreneurship and Sustainability Issues*, 5(3), 528-541.

Maria, S. (2025). Navigating the Ethical and Legal Frontiers of Hyperpersonalization in the Digital Age. Available at SSRN 5394529.

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.

Pandey, D. (2025). AI-Driven Consumer Behavior and. *Adapting Global Communication and Marketing Strategies to Generative AI*, 113.

Parshetty, H., Palimkar, L., & Emandi, R. Customer Targeting and Segmentation. In *Predictive Analytics and Generative AI for Data-Driven Marketing Strategies* (pp. 68-81). Chapman and Hall/CRC.

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

Perakakis, E., Mastorakis, G., & Kopanakis, I. (2019). Social media monitoring: An innovative intelligent approach. *Designs*, 3(2), 24.

Philip, K., Hermawan, K., & Iwan, S. (2017). Marketing 4.0: Moving from traditional to digital.

Rachmad, Y. E. (2025). Personalized Digital Influence Theory. *United Nations Economic and Social Council*.

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.

Salih, L., Tarhini, A., & Acikgoz, F. (2025). AI-Enabled service continuance: roles of trust and privacy risk. *Journal of Computer Information Systems*, 1-16.

Saura, J. R. (2024). Algorithms in digital marketing: Does smart personalization promote a privacy paradox?. *FIIIB Business Review*, 13(5), 499-502.

Sheil, A., Acar, G., Schraffenberger, H., Gellert, R., & Malone, D. (2024, May). Staying at the roach motel: Cross-country analysis of manipulative subscription and cancellation flows. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (pp. 1-24).

Singh, A., & Kakkar, A. (2025). Marketing in the age of hyper-personalisation: Lessons from analytics-driven brand success. *Applied Marketing Analytics*, 11(1), 72-86.

Sirur, S., Nurse, J. R., & Webb, H. (2018, January). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd international workshop on multimedia privacy and security* (pp. 88-95).

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/>

Ullagaddi, P. (2024). GDPR: Reshaping the landscape of digital transformation and business strategy. *International journal of business marketing and management*, 9(2), 29-35.

Yaghmourian, S. G. (2024). *The Impact of AI-Driven Hyper-Personalization on Online Purchasing Intention: The Mediating Role of Privacy Concerns* (Master's thesis, Princess Sumaya University for Technology (Jordan)).

Zehnle, M., Hildebrand, C., & Valenzuela, A. (2025). Not all AI is created equal: A meta-analysis revealing drivers of AI resistance across markets, methods, and time. *International Journal of Research in Marketing*.

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.