Ethical Concerns Surrounding User Data Privacy in Programmatic Advertising and Targeted Marketing

In our current digitalized era, user data serves as a driving economic resource in targeted marketing, and programmatic advertising has come to dominate the online advertising sphere. Defined as the combined use of data, automated technology, and advanced software that enables marketers to make real-time decisions about advertisements delivered to consumers, programmatic advertising comprised 83.9% of total U.S. display advertising spending in 2019 and is expected to only grow further *(Cooper et al., 2023)*. This sophisticated collection and application of user data in targeted advertising provides increased consumer benefits through personalized product offerings and greater relevancy in marketing communications, but also raises a range of ethical concerns surrounding user data privacy *(A Customer-Centric Approach to Marketing in a Privacy-First World, n.d.)*. These ethical implications can be investigated through the trade-off between effective marketing techniques and privacy violations, where there exists a conflict between consumers' simultaneous desires for personalized communications and greater privacy. These concerns are also reflected in the digital privacy paradox *(Martin & Murphy, 2017)*, where users claim to be concerned about their privacy, but nevertheless undertake very little to protect their personal data and relinquish private information online.

A common definition of information privacy is "the ability of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others," where users can exercise their right and ability to control the flow of information about them *(Boerman & Smit, 2023)*. However, in the context of programmatic advertising, users and advertising entities are both active participants in the sharing and collection of data to third party businesses, where it becomes difficult to precisely control what information is disclosed to others. Thus, consumer privacy in the realm of targeted marketing can also be analysed from the lens of contextual integrity, which states that the right to privacy is "neither a right to secrecy nor a right to control, but a right to appropriate flow of personal information *(Bleier et al., 2020)*." This perspective suggests that to preserve privacy, consumers do not necessarily need absolute or explicit control over their data, as long as information flows remain appropriate throughout the collection, application, and dissemination process in adherence to entrenched norms. However, technological advancements have led to a rise in products equipped with sensors and features that can ubiquitously track consumers' everyday life, allowing user information to be exploited in new contexts, potentially threatening these

societal norms and instigating privacy concerns. For example, personal health or fitness trackers often feed consumer data directly into "the cloud" to facilitate consumer activity dashboards and peer comparisons *(Bleier et al., 2020)*. Yet if this data is utilized for purposes other than fitness tracking, such as insurance or credit scoring by businesses to create targeted advertisements, information flow is disrupted into a new context, raising ethical concerns surrounding user data privacy.

There are also ethical implications in the algorithmic profiling process of targeted marketing, where consumer identities are often reduced and reshaped through algorithmic sorting and auditing techniques in data collection. Algorithmic profiling is employed in programmatic advertising to create personalized marketing by profiling consumers into different categories, including gender, age, ethnicity, lifestyle, consumption preferences, language, location, political leanings, income, employment, and marital status *(Kant, 2021)*. However, this targeting can lead to a range of racialized, socioeconomic, and gendered discrimination in data collection. In 2019, the U.S. National Fair Housing Alliance sued Facebook for providing an option for "advertisers to exclude families with children and women from receiving advertisements, as well as users with interests based on disability and national origin *(Kant, 2021)*." Similarly, in 2018, the American Civil Liberties Union and ProPublica found that job advertisements for taxi drivers, roofers, and housing removalists on Facebook were oftentimes only targeted towards male users. Consequently, Facebook has since introduced a new non-discrimination policy that disallows the use of their audience selection tools to "target" specific groups or "exclude" certain groups from seeing advertising content. Similarly, Google has announced a move away from "individualized targeting" towards "group targeting" and introduced stricter political advertising rules that restrict microtargeting. However, the notion of targeting inherently involves classifying and distinguishing audiences, so in essence, all forms of targeting can be considered exclusionary. These ethical implications are also reflected in the term "pattern discrimination" from an algorithmic and computation perspective, which describes the imposition of identifiers on input data to filter or discriminate information, rooted in existing sociocultural and economic inequalities, oftentimes eugenic and segregationist *(Kant, 2021)*. Additionally, computationally categorizing users as "male," "female," "high cost," or "celebrity," can reductively produce, govern, and (re)shape selfhood, diminishing the identity of the user into a single line of a database entry *(Kant, 2021)*.

Ethical concerns surrounding user data privacy in programmatic advertising can also be examined from a legal and business perspective, focusing in particular on the auction-based model of the online advertising ecosystem itself. This ecosystem is built upon complex interactions amongst a myriad of different

consumer and producer parties, as well as intermediary advertising companies, networks, and exchanges, making it incredibly difficult to control the flow of user data collection, application, and dissemination; webpage publishers themselves are oftentimes even unaware of what specific advertisements are shown to visiting users *(Estrada-Jiménez et al., 2017)*. User data is also processed and distributed at extremely high speeds due to real-time requirements of the online advertising marketspace, increasing the difficulty for advertising companies to anonymize and protect this data immediately after collection *(Estrada-Jiménez et al., 2017)*. There are consequently ethical implications surrounding user data privacy threats, such as data leakages, unauthorized collection of data, and privacy attacks. This business model also raises ethical concerns surrounding the potential oligopolization and collusion between large advertisement housing platforms that control vast amounts of consumer data. There exist ethical implications in targeted marketing of price discrimination and consumer exploitation, where users can be unknowingly guided to purchase products at higher prices through product steering and nudge marketing *(Bonatti, 2023)*, simply based upon their limited accessibility to personalized advertisements as a result of their algorithmic profile and recorded data.

There are also ethical concerns in programmatic advertising regarding whether users truly possess informed consent and have power to control their data privacy online. Although some consumers choose to utilize transparency and protection tools while browsing online, advanced mechanisms such as agent strings are currently implemented within the programmatic advertising ecosystem to counteract cookie removals or advertisement blocking *(Estrada-Jiménez et al., 2017)*. Users' capabilities are also extremely limited due to the invisible nature of transactions between different entities involved in the data collection and dissemination process. Consumers are oftentimes also bounded by limited technical knowledge, inhibiting their ability to mitigate data privacy risks *(Estrada-Jiménez et al., 2017)*. These restrictions are simultaneously intertwined with the risk of consumers falling into the transparency paradox *(Bleier et al., 2020)*, where information disclosures provided to them regarding data collection are either so simple as to be incomplete or deceptive, or complex as to be entirely incomprehensible. These sentiments are all reflected in concepts of privacy fatigue and privacy cynicism, where consumers feel increasingly vulnerable and powerless with their inability to control personal information, and mistrust the platforms and companies that handle their data *(Boerman & Smit, 2023)*. Many consumers do not read website privacy terms and conditions before accepting them, simply because they feel resigned to online tracking and perceive it as being ubiquitous or unavoidable *(Kant, 2021)*. These concerns also allude to the ethical principle of Respect for Persons from the Belmont Report, which emphasizes the importance of ensuring individuals freedom to act autonomously based on their own considered deliberation and

judgements, alongside the significance of informed consent and defending autonomy of those with diminished consent. However, user data privacy in programmatic advertising and targeted marketing raises issues on whether consumer agency and informed consent truly exist for users with their lack of control over the potential exploitation of personal data.

Ultimately, programmatic advertising and targeted marketing in our modern digitalized world raises a range of ethical concerns surrounding user data privacy, reflected in the trade-off between effective marketing techniques and privacy violations. These ethical implications can be explored from a variety of perspectives including algorithmic profiling and pattern discrimination in data collection, as well as the complex auction-based model of the online advertising ecosystem itself with potential for price discrimination and collusion from large advertisement housing platforms. Programmatic advertising also raises ethical concerns regarding whether users truly possess informed consent and have power to control their data privacy online, explored through lenses of the transparency paradox and privacy cynicism. While the sophisticated collection, application, and dissemination of user data in targeted advertising provides increased consumer benefits through personalized product offerings and greater relevancy in marketing communications, its consequent range of ethical implications surrounding user data privacy must also be addressed.

References:

A customer-centric approach to marketing in a privacy-first world. (n.d.). https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/a-customer-centric-approach-to-marketing-in-a-privacy-first-world

Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, *37*(3), 466–480. https://doi.org/10.1016/j.ijresmar.2020.03.006

Boerman, S. C., & Smit, E. G. (2023). Advertising and privacy: an overview of past research and a research agenda. *International Journal of Advertising*, *42*(1), 60–68. https://doi.org/10.1080/02650487.2022.2122251

Bonatti, A. (2023, May 23). *The Platform Dimension of Digital Privacy | NBER*. https://www.nber.org/books-and-chapters/economics-privacy/platform-dimension-digital-privacy

Cooper, D. A., Yalcin, T., Nistor, C., Macrini, M., & Pehlivan, E. (2023). Privacy considerations for online advertising: a stakeholder's perspective to programmatic advertising. *Journal of Consumer Marketing*, *40*(2), 235–247. https://doi.org/10.1108/JCM-04-2021-4577

Estrada-Jiménez, J., Parra-Arnau, J., Rodríguez-Hoyos, A., & Forné, J. (2017). Online advertising: Analysis of privacy threats and protection approaches.

Computer Communications, *100*, 32–51.
https://doi.org/10.1016/j.comcom.2016.12.016

Kant, T. (2021). Identity, Advertising, and Algorithmic Targeting: Or How (Not) to Target Your "Ideal User." *MIT Case Studies in Social and Ethical Responsibilities of Computing.* https://doi.org/10.21428/2c646de5.929a7db6

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155.
https://doi.org/10.1007/s11747-016-0495-4